PLANET Mesh Network

MAP-2000 / MAP-2000R
MAP-2100

Web Based Management
&
User Manual

Rev 1.0

Table of Content

1 Introduction 4

2 Web based management 7

2.1 To start the Web based configuration 7

2.2 Web based configuration menu overview 9

2.2.1 Configuration Menu 9
2.2.2 Command Menu 11
2.2.3 Info 11
2.2.4 Links Menu 11

2.3 Configuration Menu 12

2.3.1 Configuration->System Settings 12
2.3.2 Configuration->Network->WAN 13
2.3.3 Configuration->Network->Local Network 16
2.3.4 Configuration->Network->WLAN 16
2.3.5 Configuration->Network->Node to Node 19
2.3.6 Configuration->Network->Route 22
2.3.7 Configuration->Security->MAC Filter 23
2.3.8 Configuration->Security->Authentication 26
2.3.9 Configuration->Local Services->DHCP-Server 30
2.3.10 Configuration->Local Services->Firewall 32
2.3.11 Configuration->Local Services->NAT 36
2.3.12 Configuration->Local Services->VPN Server 38
2.3.13 Configuration->Local Services->NTP-Client 38
2.3.14 Configuration->Local Services->QoS 40
2.3.15 Configuration->Local Services->Traffic Shaping 41
2.3.16 Configuration->System Management->Password 42
2.3.17 Configuration->System Management->SNMP 43
2.3.18 Configuration->System Management->Remote-Syslog 44
2.3.19 Configuration->Login Setup->Login Parameters 44
2.3.20 Configuration->Login Setup->Radius 49
2.3.21 Configuration->Login Setup->Local Users Database 51
2.3.22 Configuration->Login Setup->Customize 52
2.3.23 Configuration->Login Setup->Webspace 60
2.3.24 Configuration->Tools->Ping 60
2.3.25 Configuration->Tools->Download 62
2.3.26 Configuration->Tools->Firmware Update 62
2.3.27 Configuration->Tools->Settings 64

2.4 Command Menu 66

2.4.1 Command->Reboot 66
2.4.2 Command->Reset 66

2.5 Info Menu 67

2.5.1 Info->Status->System 68
2.5.2 Info->Status->Interfaces 69
2.5.3 Info->Status->Services 71
2.5.4 Info->Status->Users 72
2.5.5 Info->Status->Mobile IP 72
2.5.6 Info->Topology 72
2.5.7 Info->Route 73
2.5.8 Info->Syslog 75

2.6 Links 76

3 Logging in through MESH AP 77

Step 1: User Starts WEB Browser 77

Step 2: Login Page Presented to User 77
Step 3: User Supplies Credentials 78
Step 4: User Login Success 78
Step 5: Display the Request Home Page 78
Step 6: User Logout 79

1 Introduction

PLANET Mesh Network features with a Web-based configuration interface management tool. It provides an easy access to all configuration functions.

Any computer either wired or wireless that establishes a valid connection with the MESH AP can access the web-based configuration through a web browser.

For the first time configuration, the MESH AP can be configured with a wireless computer, equipped with wireless LAN adapter or a PC equipped with wired Ethernet card and crossover Ethernet cable to the MESH AP's Ethernet port. For more detail, please also refer to the Quick Guide.

- For the wireless computer that equipped with 802.11b/g wireless LAN adapter, the following settings are required to ensure a successfully connection to the MESH AP.
    - ESSID: PLANET
    - WEP: disabled
    - TCP/IP installed and enable DHCP (Dynamic IP)

- For the computer that equipped with wired Ethernet card and crossover cable to the MESH AP's LAN port.
    - TCP/IP installed and enable DHCP

- The preset MESH AP administrator login user ID and password is '**admin**'.

After the first time configuration, the MESH AP can be managed either locally or remotely. For local management, computer can connect to the MESH AP by wireless interfaces to MESH AP wireless interface or wired LAN interface with crossover cable to MESH AP LAN port. For remote management, a VPN connection to MESH AP via the Internet can manage the MESH AP remotely.

The following are all MESH AP default settings:

- Configuration
    - System
        - System
            - Node Name: PLANET
            - Contact Name:
            - Contact Phone:
            - Contact Email:
            - Object ID: 1.3.6.1.4.1.10456.6.3.1.0
    - Network
        - WAN
            - Interface Type: DHCPC
        - Network
            - Enable DNS Client : enabled
            - DNS Client Default Domain Name : PLANET
        - Bridge
            - IP Address: assigned automatically
            - Netmask: assigned automatically
        - WLAN
            - WLAN0

- SSID: PLANETMeshNet
- Radio role: Mesh
- Rate profile: Auto
- Frequency channel : 7
- Auto channel selection: disabled
- Transmit power : Max

- WLAN1
  - SSID: PLANET
  - Broadcast SSID: disabled
  - Radio role: Access Point
  - Rate profile: Auto
  - Frequency channel : 1
  - Auto channel selection: enabled
  - Transmit power : MAX

- NODE
  - Auto IP configuration : enabled
  - Traffic encryption :disabled
  - Enhanced traffic encryption: disabled
- Route
  - Static Routing: disabled

- Security
  - MAC Access
    - MAC Access control : disabled
  - Encryption
    - Encryption: disabled
    - Authentication type: open
    - Deny non-encrypted data: disabled
  - Authentication
    - Mode: None
- Services
  - DHCP-Server
    - DHCP-Server: enabled
    - Subnet Mask: assigned automatically
    - Gateway IP Address: assigned automatically
    - Primary DNS IP Address: assigned automatically
    - DHCP Domain : PLANET
    - IP Pool Table: assigned automatically
  - Firewall
    - Mode: Disabled
  - NAT
    - Mode : Enabled
  - NTP-Client
    - Mode: Disabled
  - QoS
    - Mode: Enabled
    - Default Upload : 256
    - Default Download :256
- Management
  - Webbased password
    - Username: admin
    - Password: admin

- SNMP Password
  - SNMPv2 Read Password: public
  - SNMPv2 Read/Write Password: private
  - SNMPv3 Read Password: snmpv3rouser
  - SNMPv3 Read/Write Password: snmpv3rwuser
  - SNMPv3 Secret Password: snmpv3password
  - SNMPv3 Secret Passphrase: snmpv3passphrase
- Remote-Syslog
  - Mode: Disabled

o Login Setup
- Login
  - Require User Login: enabled
  - Idle timeout: 300
  - Login method: http and https
- Radius
  - NAS-Identifier: PLANET
  - Called-Station ID: PLANET
  - NAS-Port :1
  - NAS-Port-Type: 19
  - Primary authentication port :1812
  - Primary accounting port :1813
  - Secondary authentication port:1812
  - Secondary accounting port: 1813
  - Interim-Update Interval:180
- Local Users
  - No users enrolled

2 Web based management

2.1 To start the Web based configuration

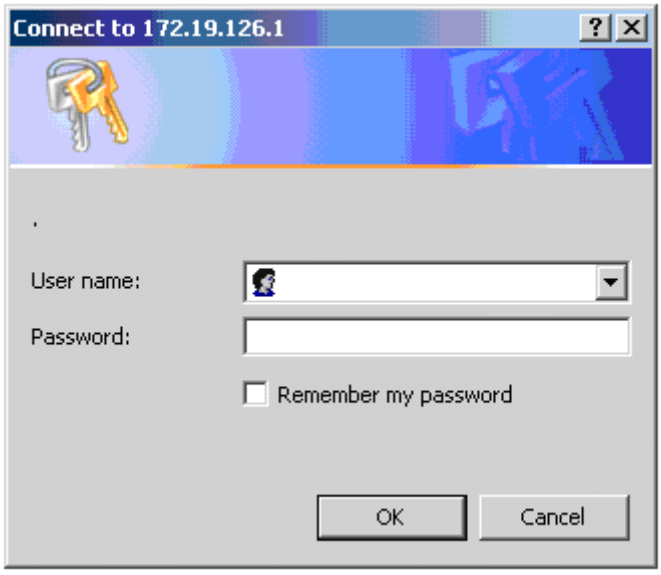
a. Start the web browser

b. Enter https://IP Address of the MESH AP, in the address box (make sure HTTPS, but not HTTP)

c. Accept the security certificate and click 'Yes' to proceed.

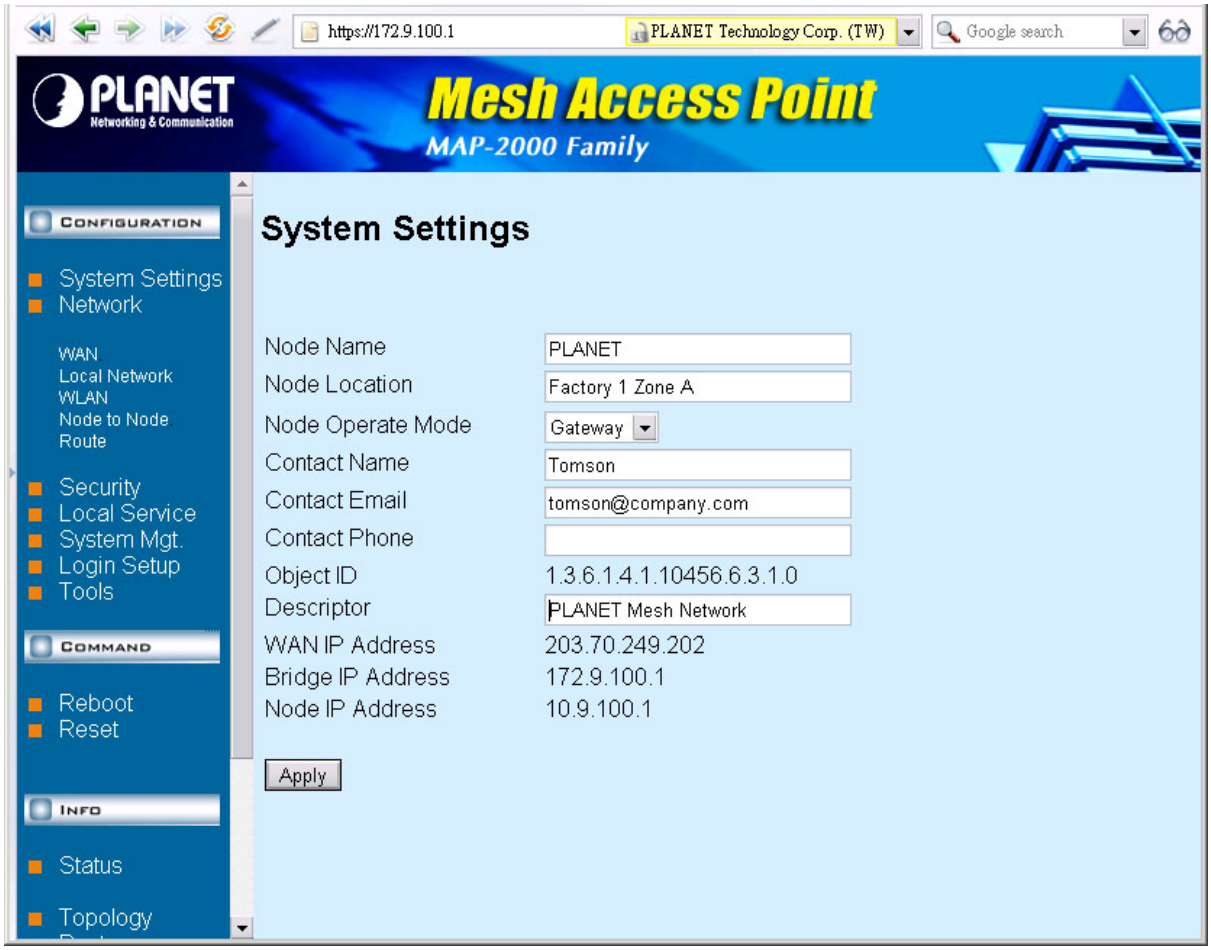
Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
The security certificate date is valid.
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

d. The Web-based configuration login page opens after the security certification has been accepted.



e. Enter the user name and password. By default, the user name and password are both set to '**admin**'.

f. After login successfully, the Web-based configuration main page is open, which is appealed as below.



2.2 Web based configuration menu overview

This section gives a brief summary to the menu options of the Web-based configuration.

2.2.1 Configuration Menu

- This menu allows the administrators to configure the various MESH AP settings, including network setting, VPN server setting, WLAN interface setting and so on.

- Comprise of seven different submenu
  - System Settings
    - Contains the setting of general info and operation mode of the device
    - Contains options to fine tuning the network operations.
    - Contains the following submenu:
      - WAN
        - To select and configure the WAN connection interface
        - To specific the basic network configuration such as hostname, domain etc.
      - Local Network
        - To specific the address of local network.
      - WLAN
        - To configure the WLAN interfaces settings such as ESSID, data rate, channel.
      - Node to node
        - To configure the node configuration such as node ip.
      - Route
        - To modify the network routing table
  - Security
    - Contains option to configure the type of security
    - Contains the following submenu:
      - MAC Access
        - To specific the access control rule based on the MAC address
      - Authentication
        - To specific the type of authentication such as WEP, 802.1x, and 802.11i
  - Local Service
    - Contain the options to configure the various network services such as DHCP server, firewall, VPN server , etc
    - Contains the following submenu:
      - DHCP-Server
        - To configure the MESH AP to act as a DHCP server to the bridge interface
        - To specify fixed IP address
      - Firewall

        - To specific the firewall rules and settings to protect the WAN port
    - NAT
        - To specific the Network Address Translation (NAT) rule and let user to define static routes to make computers on the internal network (LAN/WLAN) visible to external computers
    - VPN Server
        - To configure VPN server to make remote management available with enhanced security
    - NTP-Client
        - To synchronize to the specified NTP (Network Time Protocol) server and let NTP server to control system time
    - Remote-Syslog
        - To track and log system messages to a remote syslog server
    - QoS
        - To prioritize packet based on TCP,port,size of packet
    - Traffic Shaping
        - To configure the upload and download bandwidth of the users
    - Mobile IP
        - To configure mobile IP for the current nodes
- System Mgmt
    - To manage configurations and firmware file and control the administrator login password
    - Contains the following submenu
        - Password
            - To change the administrator login password
        - SNMP
            - To change the snmp password
        - Syslog Server
            - To configure the remote syslog parameter
- Login Setup
    - Contains the following submenu:
        - Login
            - To specific the login method
        - RADIUS
            - To define the RADIUS client settings that need to login to the external RADIUS server
        - Local Users Database
            - To define the local user accounts that allow to access.
        - Customize
        - Webspace
- Tools
    - Contains the following submenu
        - Ping
        - Download
        - Firmware Update
        - Settings

2.2.2 Command Menu

- This menu allows the administrators to do certain commands such as download, reboot, reset and help links.
- Comprise of two different submenu
    - Reboot
        - To reboot the MESH AP
    - Reset
        - To restore the default factory setting of MESH AP

2.2.3 Info

- This menu allows the administrator to view the current status of different components of the MESH AP. And, to provide diagnostic tools to investigate the MESH AP behaviors.
- Comprise of three different submenu
    - Status
        - To show the current status of different component of MESH AP
        - Contains the following submenu
            - System
                - To show the current system uptime, CPU and memory status
            - Interfaces
                - To show the information of WAN, LAN and WAN physical interfaces
            - Services
                - To show the current status of various services available on the MESH AP
            - Users
                - To show the list of online users and their detail information that had login to the MESH AP successfully
    - Topology
        - To provide a simple topology overview of the mesh network.
    - Route
        - Display the information of routing table inside the system
    - Syslog
        - Display the log messages from the system

2.2.4 Links Menu

- This menu provides the HTML links to the MESH AP main webpage and PLANET homepage

2.3 Configuration Menu

This section explains the detailed settings and options provided by the Configuration Menu. Configuration menu allows the administrators to configure the various settings, including network setting, VPN server setting, WLAN interface setting and so on.

Configuration menu consists of seven different submenus. They are known as system settings, network, security, local services, system management, login setup and tools. Each submenu has its own options to provide complete configuration settings. Figure below shows the main page of the Configuration Menu.

2.3.1 Configuration->System Settings

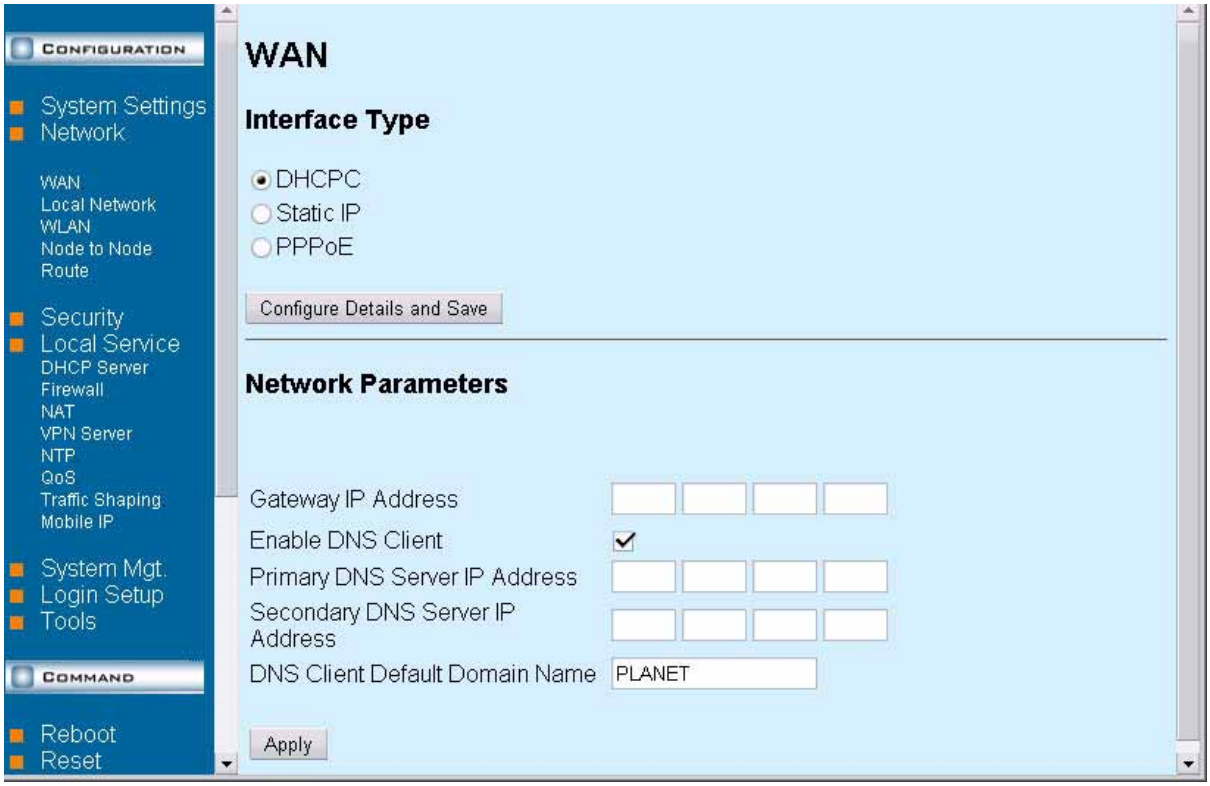
Administrator also can assign name and location to MESH AP for better management.
System parameters:

- Node Name
  - To specify the name of the node
  - Example: PLANET
- Node Location
  - To specify the location of the node
  - Example: Factory 1, Zone A, Ivy road, …
- Node Operate Mode
  - Display the operation mode of current node
    For MAP-2000 / MAP-2100, Gateway or Relay
    For MAP-2100, only fixed at Relay mode
- Contact Name
  - To specify the name of contact for assistant for the node
  - Example: John, Tomson, ….
- Contact Phone

  - To specify the phone number of the contact person
- Contact Email
  - To specify the email of the support person
  - Example: support@abc.com
- Object ID
  - Display the object ID of the system
- WAN IP Address
  - Display the WAN IP address of the system
- Bridge IP Address
  - Display the Bridge IP of the system
- Node IP Address
  - Display the Node IP of the system
- Descriptor
  - To specify the description of the system

2.3.2 Configuration->Network->WAN

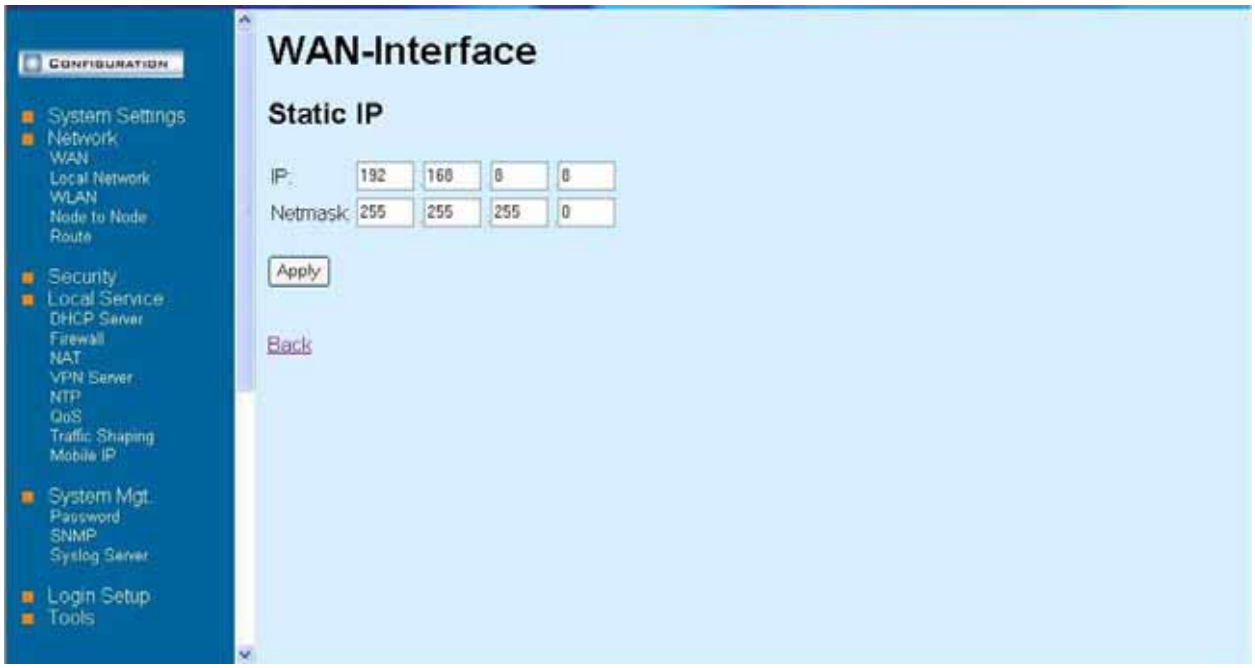
This submenu defines the configuration of WAN port interface. Three options are available to configure the WAN port interface to connect to the Internet. They are known as DHCPC (Dynamic Host Configuration Protocol client), Static IP and PPPoE (Point to Point Protocol over Ethernet). Network parameters are for the configurations of gateway IP, DNS IP.



WAN-Interface Parameters:

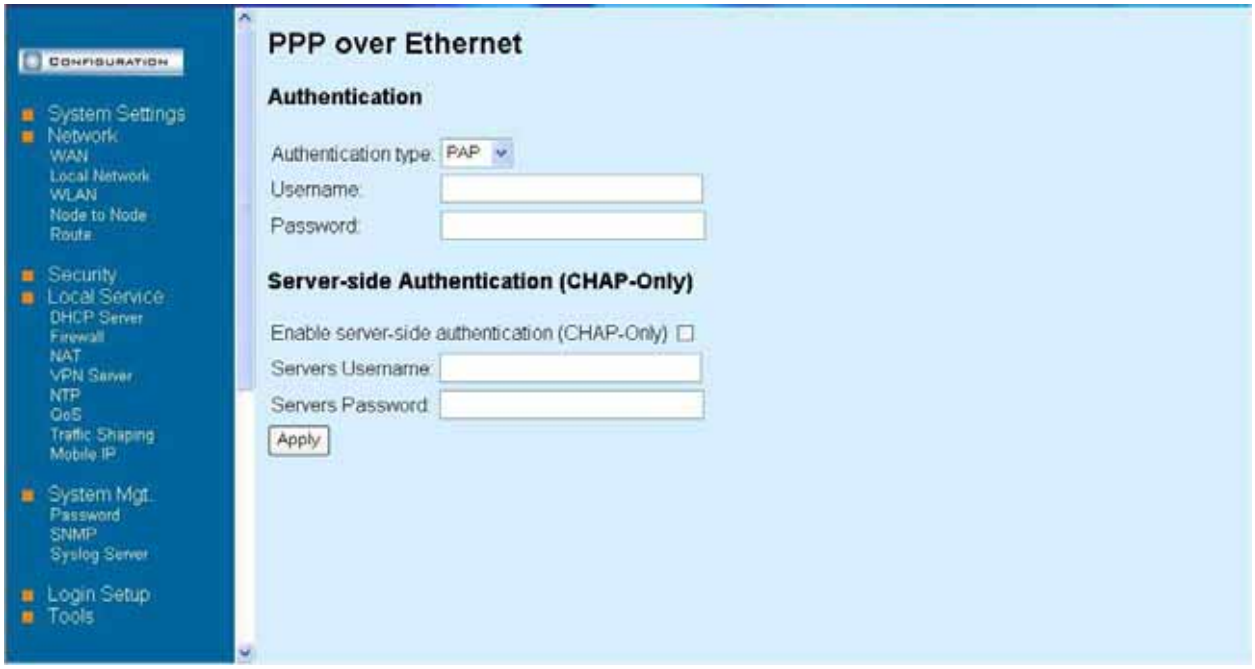
- Interface Type->DHCPC
  - The ISP's DHCP server automatic assigns an IP address to the WAN interface.
  - To select DHCP client option, click the DHCPC radio button
  - Click "Configure Details and Save" button to configure that option

- Interface Type->Static IP
  - To manually assign a fixed IP address to the WAN interface
  - To select the Static IP option, click the Static IP radio button
  - Click “Configure Details and Save” button to configure that option



  - Static IP Parameters:
    - IP
      - To specific the IP address of the WAN-interface
    - Netmask
      - To specific the network mask of the static IP address
    - Click “Save Config” to save the configuration changed

- Interface Type->PPPoE
  - ISP assigns a valid IP address to the WAN interface after MESH AP logon to the ISP’s PPPoE with supplied valid username and password.
  - To enhance to network security, MESH AP supports server side authentication feature. PPPoE server needs to supply valid username and password to authenticate itself. Only CHAP (Challenge Handshake Authentication Protocol) is supported for this feature.
  - Two authentication types are supported in the PPPoE mode, i.e. PAP (Password Authentication Protocol) and CHAP (Challenge Handshake Authentication Protocol). Only CHAP (Challenge Handshake Authentication Protocol) is supported in the Server Side Authentication feature.
  - To select the PPPoE option, click the PPPoE radio button
  - Click “APPLY” button to configure that option



- PPP over Ethernet Parameters:
  - Authentication
    - Authentication type
      - To select the PPPoE authentication type, either CHAP (Challenge Handshake Authentication Protocol) or PAP (Plain Text Authentication Protocol)
    - Username
      - To specify the PPPoE logon user name
    - Password
      - To specify the PPPoE logon password
  - Server-side Authentication (CHAP-Only)
    - Enable server-side authentication
      - To enable or disable this option
    - Servers username
      - To specify the server username
    - Servers password
      - To specify the server password
  - Click “Apply” to save the configuration changed

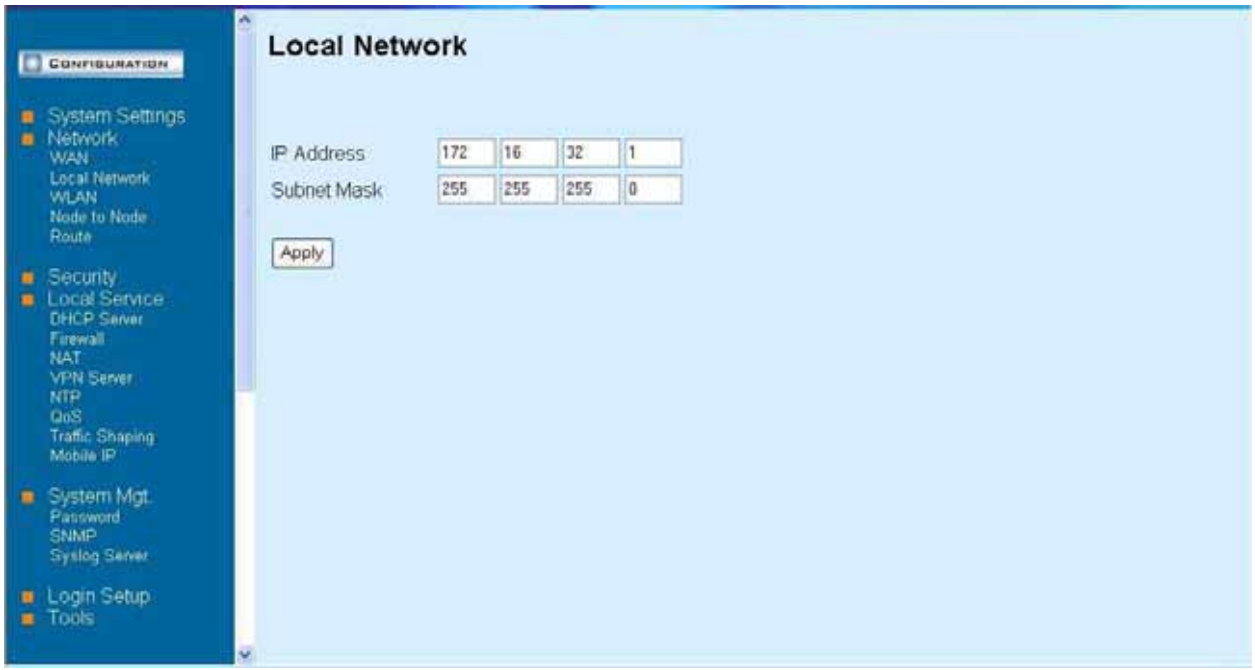
Network Parameters:

- Gateway IP Address
  - Specify the IP address of the default gateway
- Enable DNS Client
  - Enable or disable the DNS Client
- Primary DNS Server IP Address
  - Specify the IP address of primary domain name server
  - Example: 168.95.1.1
- Secondary DNS Server IP Address
  - Specify the IP address of secondary domain name server
  - Example: 202.188.1.5
- DNS Client Default Domain Name
  - Specify the domain name of the MESH AP
  - Default value: PLANET

- Click “APPLY” to save the configuration changed

2.3.3 Configuration->Network->Local Network

This submenu defines the IP configuration of bridge interface. MESH AP acts a bridge between wired LAN and wireless LAN. The LAN port interface shares the same IP address range with the wireless LAN interfaces. A static IP address is required on this port, because MESH AP cannot function as a DHCP client on its LAN port interface. The LAN port (for model MAP-2000R and MAP-2100) is used to connect the wired computers to the public access network via the LAN port interface.
Be reminded, for MAP-2000, the local network setting is for Wireless AP serviced network subnet only.

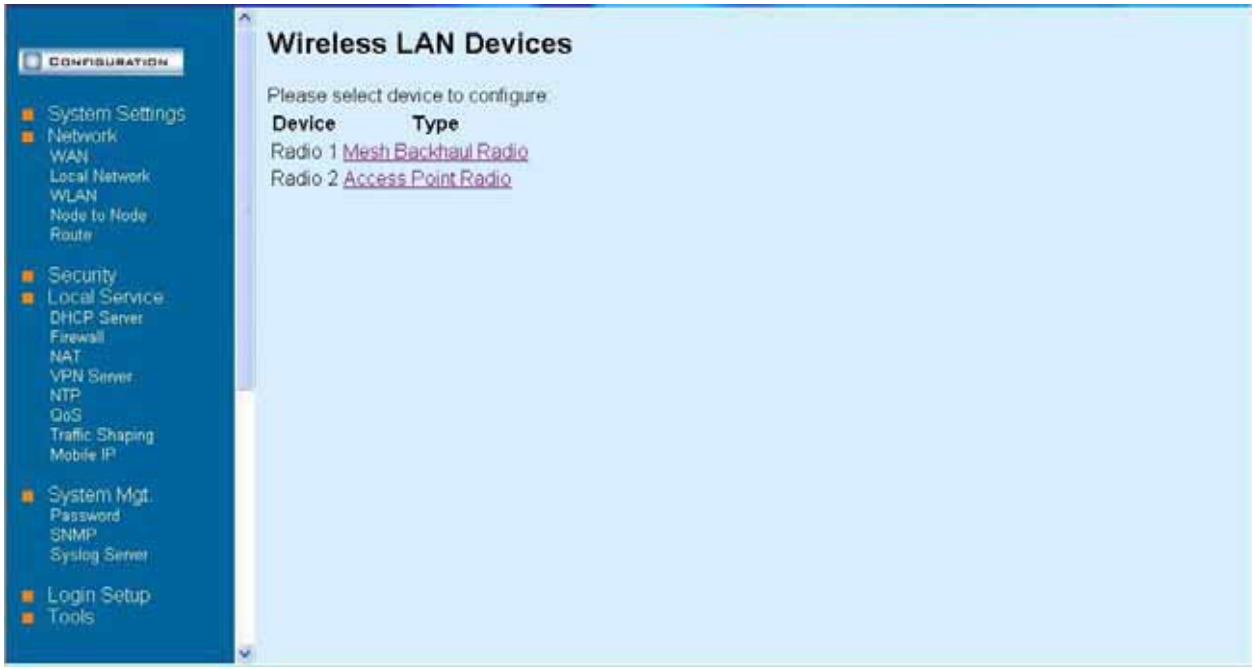


Local Network Parameters:

- IP Address
  - To specify the IP address on the bridge interface
  - Example: 172.16.1.1
- Subnet Mask
  - To specify the network mask
  - Example: 255.255.255.0
- Click “Apply” to save the configuration changed

2.3.4 Configuration->Network->WLAN

This submenu defines the configurations to the two wireless LAN interfaces embedded in the MESH AP. The WLAN LAN devices settings include the WLAN network settings such as ESSID (Extended Service Set Identifier), data rates. ESSID is the unique network name to identify the WLAN network. The data rate specifies the maximum data transfer in the WLAN network.

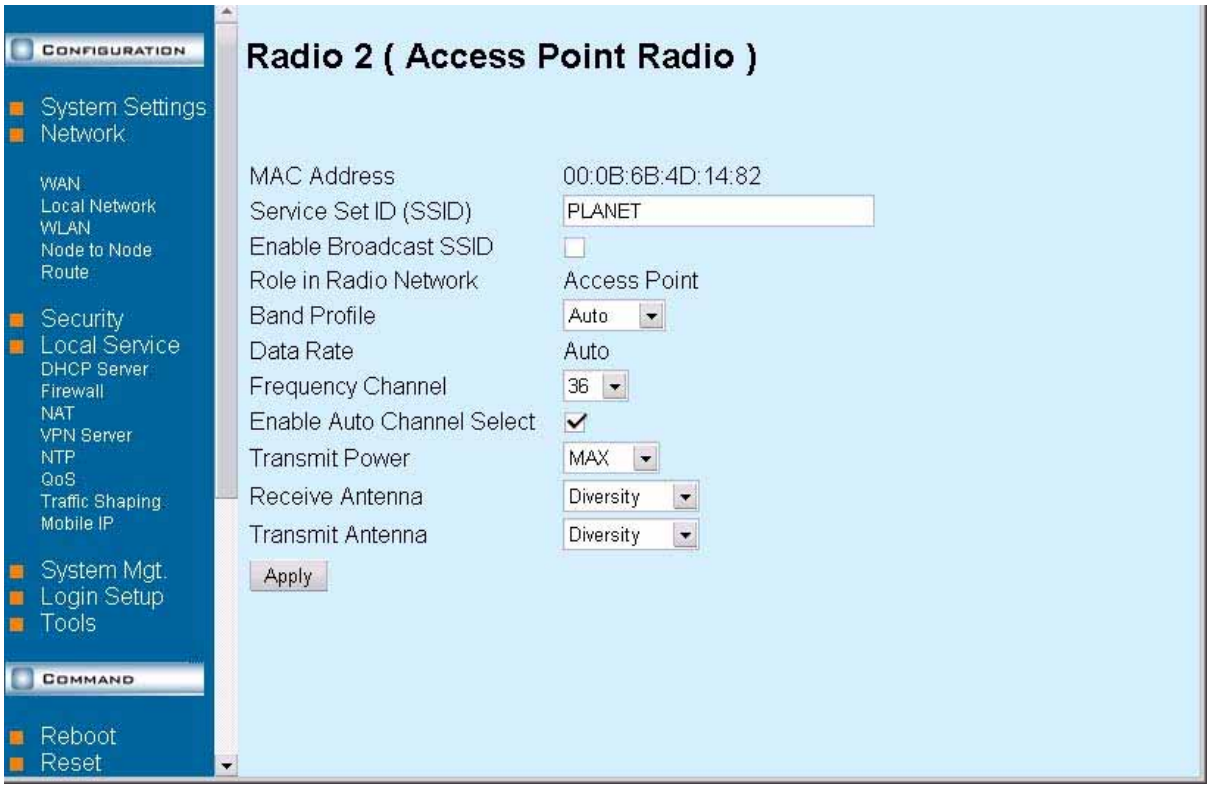


Wireless LAN Devices Parameters:

- Wireless LAN Devices
  - o List down detected WLAN devices
  - o WLAN devices are distinguished by MAC and Type
  - o Select one of the device to configure the parameters.

  - o Radio 1 (Mesh Backhaul Radio) Parameters:
    - MAC Address
      - o Display the MAC address of the devices
    - Service Set ID

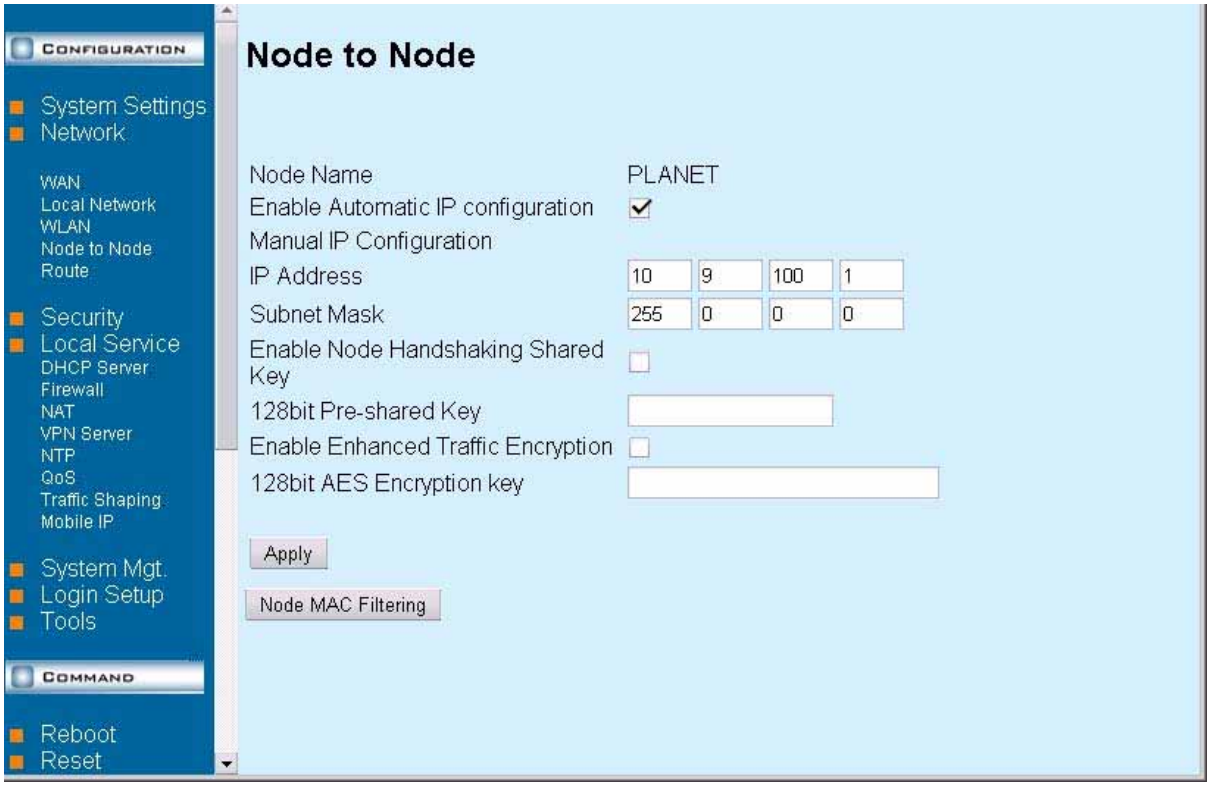
  - To specify the service set ID of the network
  - Default value: PLANETMeshNet
- Role in Radio Network
  - Display the role of radio
- Data Rate Profile
  - To configure the date rate of this device
- Frequency Channel
  - To configure the channel of this device
  - Default value: 7
- Enable Auto Channel Select
  - To enable the auto channel selection mechanism
  - Default value: disabled
- Transmit Power
  - To specify the transmit power
  - Default value: MAX
- Receive Antenna
  - To specify the diversity of the antenna
  - Default value: diversity
- Transmit Antenna
  - To specify the diversity of the antenna
  - Default value: diversity
- Country
  - To specify the regulatory domain of the radio
    Note: This value also will apply to Radio 2.
- Click “Apply” to save configuration changed



  - Wireless-Interface(Radio 2) Parameters:
    - MAC Address
      - Display the MAC address of the devices
    - Service Set ID
      - To specify the service set ID of the network

  - Default value: PLANET
- Enable Broadcast SSID
  - To enable or disable the broadcast SSID of the device
- Role in Radio Network
  - Display the role in radio network
- Data Rate Profile
  - To configure the date rate of this device
- Frequency Channel
  - To configure the channel of this device
  - Default value: 1
- Enable Auto Channel Select
  - To enable the auto channel selection mechanism
  - Default value: enabled
- Transmit Power
  - To specify the transmit power
  - Default value: MAX
- Receive Antenna
  - To specify the diversity of the antenna
  - Default value: diversity
- Transmit Antenna
  - To specify the diversity of the antenna
  - Default value: diversity
- Click “APPLY” to save configuration changed

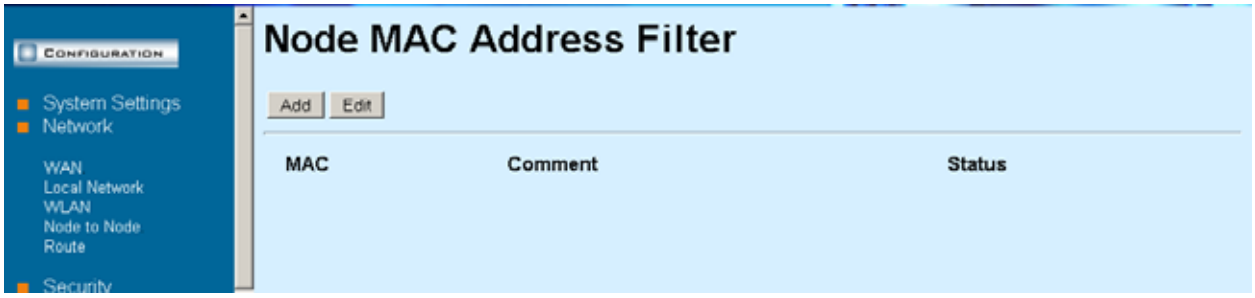
2.3.5 Configuration->Network->Node to Node



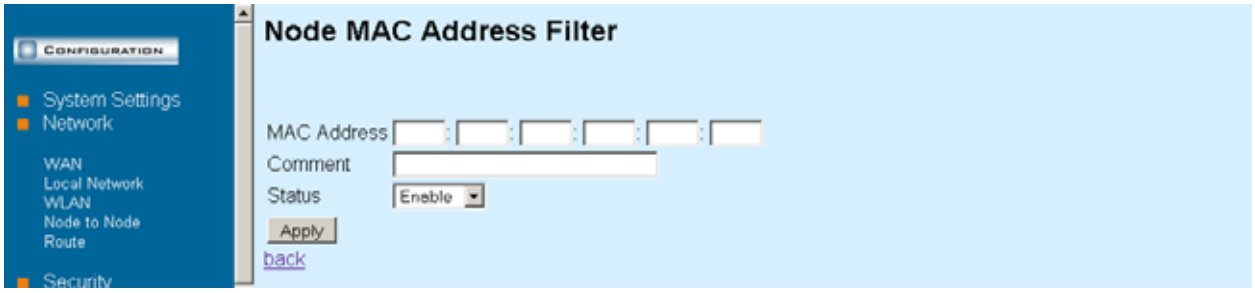
Node Parameters:

- Node Name
  - Display the name of the node

- Enable Automatic IP Configuration
  - To enable or disable the automatic IP configuration to MESH AP. This option will assign an IP address automatically based on the MAC address of the WAN devices. The assigned IP range is as follow:
    - 172.16.0.0/12 reserved for Bridge device
      - MESH AP's bridge will be assigned 172.X.Y.1
      - MESH AP's client will be assigned from 172.X.Y.2 to 172.X.Y.254
      - X & Y would be deduced from the WAN devices
    - 10.0.0.0/8 reserved for Node IP
      - MESH AP's node will be assigned 10.X.Y.1
      - MESH AP's vpn server will be assigned 10.X.Y.254
      - MESH AP's vpn client will be assigned from 10.X.Y.2 to 10.X.Y.12
    - Example: With deduced X=9 and Y=100 (from WAN MAC: 09h-64h), then MESH AP's node IP will be assigned with 10.9.100.1, the VPN server will be assigned with 10.9.100.254, the VPN client will be assigned from 10.9.100.2 to 10.9.100.12. For the bridge, it will use 172.9.100.1, and the MESH AP's client will be assigned with IP address ranging from 172.9.100.2 to 172.9.100.254 by MESH AP's DHCP server
  - Default value: enabled
- IP Address
  - To specify the IP address of the node
  - Example: 10.9.100.1; deduce from the WAN MAC address.
- Subnet Mask
  - To specify the network mask of the node
  - Example: 255.0.0.0
- Enable Node Traffic Encryption
  - To enable or disable node traffic encryption
- 128bit Encryption key
  - To specify the encryption key of node traffic in HEX value (0-9, A-F)
  - Example: 1234567890abcdef0123456789abcdef
- Enable Enhanced Traffic Encryption
  - To enable or disable enhanced traffic encryption
- 128bit AES Encryption Key
  - To specify the 128bit AES encryption key in HEX value (0-9, A-F)
  - Example:1234567890abcdef0123456789fedcba
- Click "Apply" to save configuration changed
- Click "Node MAC Filtering" to trigger the screen shot as below to set a list of MAC address that needed to be blocked from the current network.



- Click "Add" to add new entry , "Edit" to edit selected entry



- Node MAC filter parameter
  - MAC Address
    - To specify the MAC address to be filtered out from the network
  - Comment
    - To specify comments about the entry
  - Status
    - To enable or disable the current entry

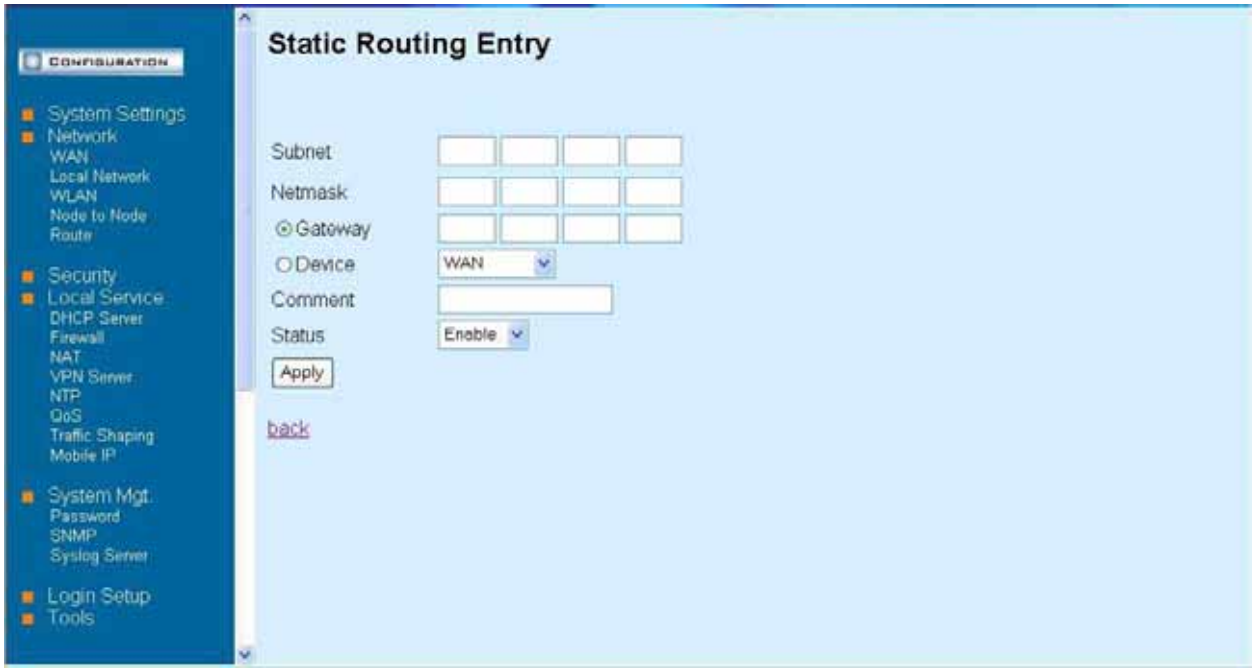
2.3.6 Configuration->Network->Route

This submenu defines the static route to direct the traffic to the appropriate destination.

Static Routing Parameters:

- Enable Static Routing
  - To enable or disable the static routing option
- Routing Table
  - To list the current routing table
- Click “Apply” to save configuration changed
- Click “Add” to add new rule to the Routing Table
- Click “Edit” to edit the selected rule

This Static routing rules will be available after either “Add” or “Edit” button is pressed.



- Static Routing Rules Parameters:
  - Subnet
    - To specify the IP subnet to be routed
    - Example: 192.168.2.0
  - Netmask
    - To specify the network mask value of the IP subnet
    - Example: 255.255.255.0
  - Gateway
    - To specify the gateway for the specified route
    - Example: 192.168.1.1
  - Device
    - To specify the interfaces for the specified route
    - Example: WAN
  - Route Using
    - To specify the route using device or gateway
    - Example: Gateway
  - Comment
    - To specify the comment for the specified route
  - Status
    - To enable or disable the specified route
  - Click “Apply” to save the configuration
  - Click “back” to go back to Configuration->Network->Route

2.3.7 Configuration->Security->MAC Filter

This submenu enable the MESH AP to control the access from the client based on the MAC address.

MAC Access Parameters:

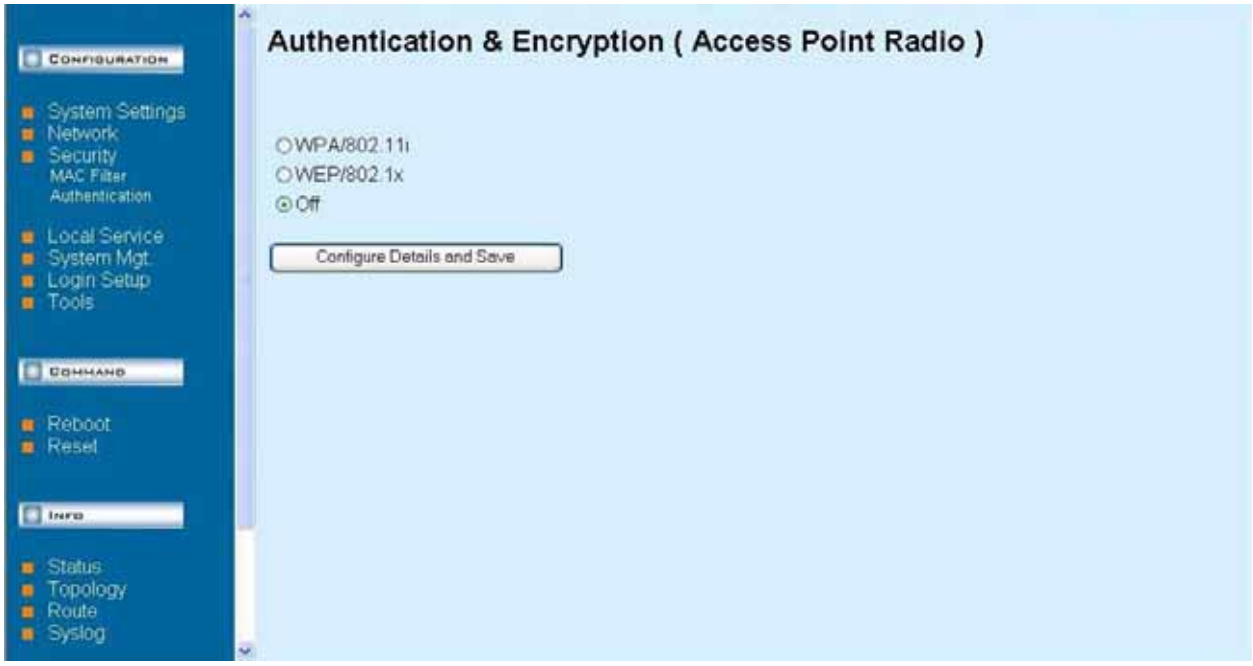
- Enable MAC Access Control
  - To enable or disable MAC access control
- Operation Type
  - To specify the type of operation of the control, ie block or pass-through
- MAC Access Control Table
  - List the MAC address configured
- Click “APPLY” to save the configuration changed
- Click “Add” to add new entry
- Click “Edit” to edit the selected entry

The MAC access control entry will be available after “Add” or “Edit” button is pressed.

- MAC Access Control entry Parameters:
  - MAC Address
    - To specify the MAC address of the entry
    - Example: 00:30:4f:08:6A:37
  - Comment
    - To specify the comment for the entry
  - Status
    - To enable or disable the entry

2.3.8 Configuration->Security->Authentication

This submenu configure the authentication method to off, WEP/802.11x, or WPA/802.11i. This security option provide more robustness in network security.



Authentication Parameters:

- To configure WPA/802.11i, click on the radio button of the WPA/802.11i

- WPA/802.11i

WPA/802.11i parameters:

- WPA PSK
  - To specify the authentication mode to WPA Pre Shared Key
- WPA EAP (RADIUS)
  - To specify the authentication mode WPA EAP, an external radius server is needed for this type of authentication
- TKIP
  - To specify the encryption cipher to Temporal Key Integrity Protocol (TKIP)
- AES
  - To specify the encryption cipher to Advanced Encryption Standard (AES)

- Available authentication mode are WPA PSK with TKIP, WPA PSK with AES, WPA EAP with TKIP, WPA EAP with AES
- Click “Save Config” to save configuration changed.

- WEP/802.1x

WEP/802.1x Parameters:

- 802.1x assignment of 128 bit key
  - To specify the authentication mode to 802.1x 128bit
- 802.1x assignment of 64 bit key
  - To specify the authentication mode to 802.1x 64bit
- 128 bit
  - To specify the authentication mode to WEP 128bit
  - Example: 01234567890abcdef1234567890
- 64 bit
  - To specify the authentication mode to WEP 64bit
  - Example: 0123456789

- Select one of the radio button to enable the authentication type.
- Click “Save Config” to save configuration changed.

- Off

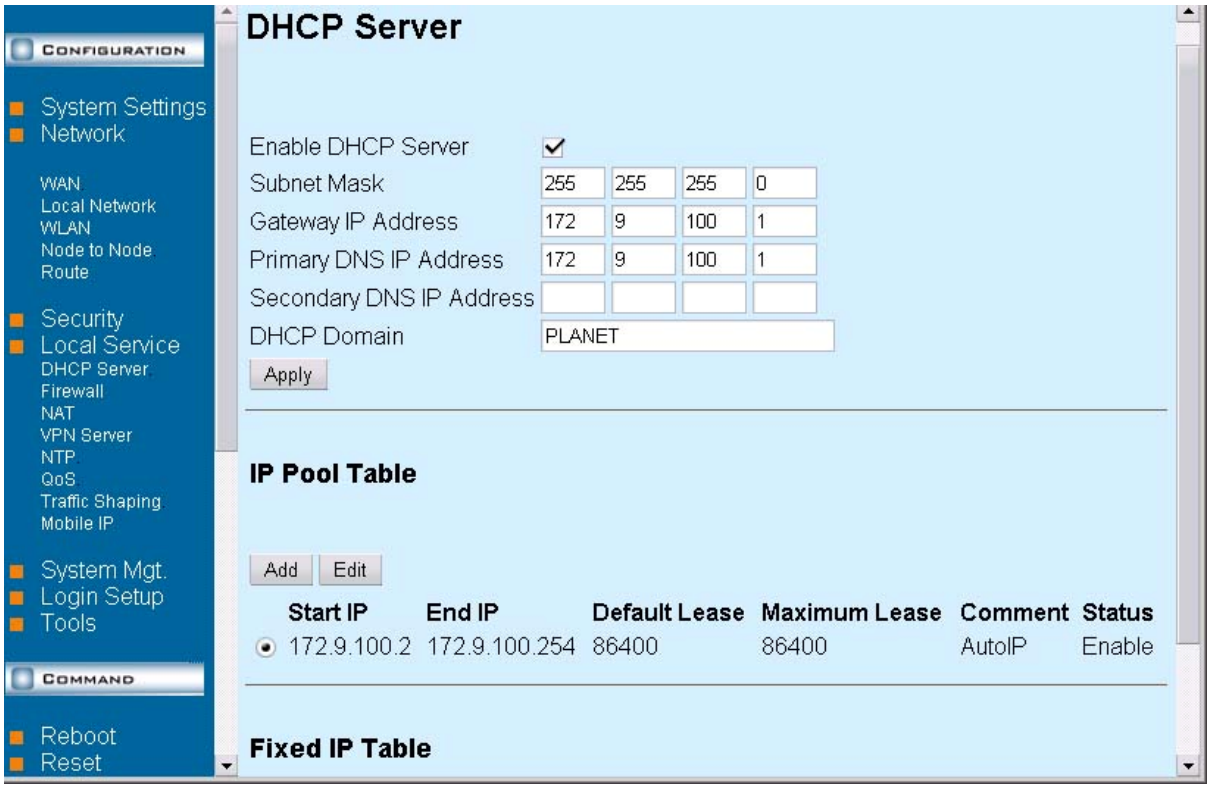
Off Parameters:

- Encryption OFF
  - To disable encryption and authentication

- Click “Encryption OFF” button to disable encryption and authentication.

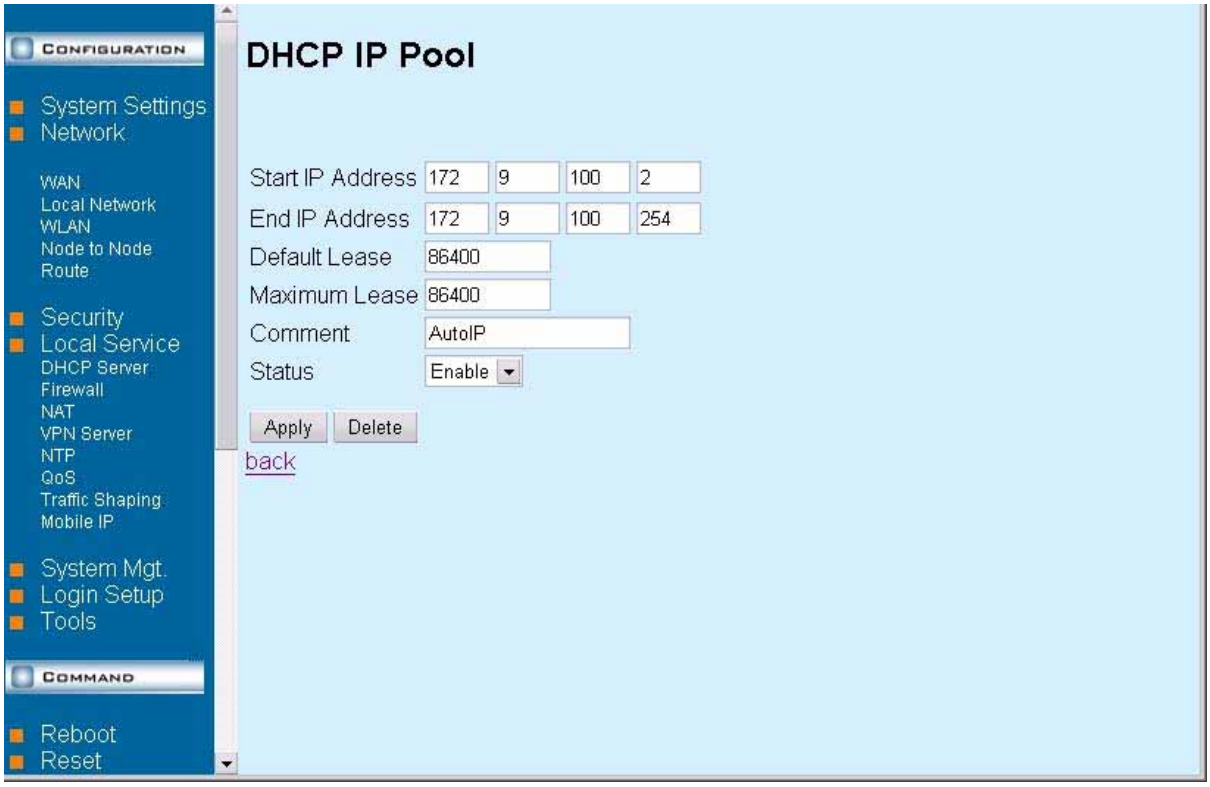
2.3.9 Configuration->Local Services->DHCP-Server

MESH AP acts as a DHCP server by default. This means it will assign IP address to client stations on Wireless and Wired network (except model: MAP-2000), up to 254 clients is supported in each node.

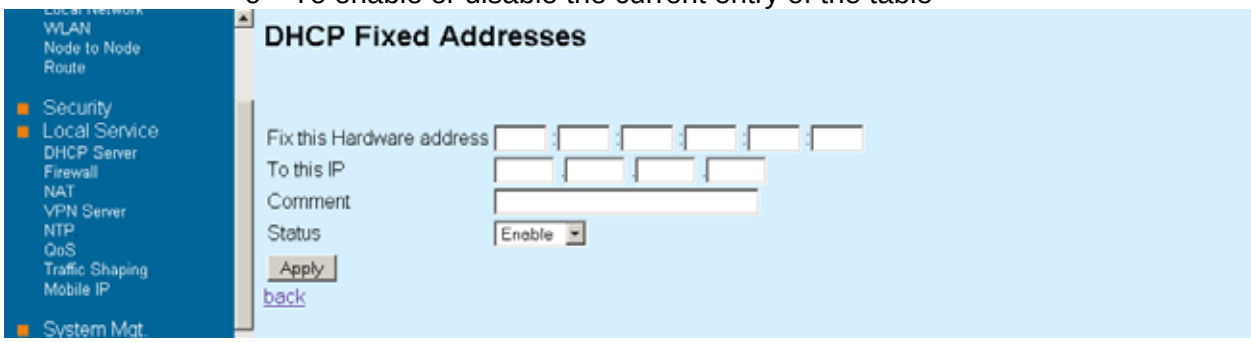


DHCP Server Parameters:

- Enable DHCP Server
  - To enable or disable the DCHP Server
  - Default value: enabled
- Subnet Mask
  - To specify the network mask of the DHCP server
  - Example: 255.255.255.0
- Gateway IP Address
  - To specify the default gateway for routing
  - Example: 172.9.100.1
- Primary DNS IP Address
  - To specify DNS server to be used
  - Example: 172.9.100.1
- Secondary DNS IP Address
  - To specify secondary DNS server to be used
- DHCP Domain
  - To specify the domain name for the DHCP clients
  - Example: PLANET
- IP Pool Table
  - A list of tables that display the IP assignment



- DHCP IP Pool Parameters:
  - Start IP Address
    - To specify the start IP of the IP pool table
    - Example: 172.9.100.2
  - End IP Address
    - To specify the end IP of the IP pool table
    - Example: 172.9.100.254
  - Default Lease
    - To specify the lease time to be assigned to the client stations
    - Example: 3600
  - Maximum Lease
    - To specify the maximum least time to be assigned to the client stations
    - Example: 86400
  - Comment
    - To specify the comments of the current entry of the table
  - Status
    - To enable or disable the current entry of the table



- DHCP Fixed Addresses Parameters:
  - Fix this Hardware address

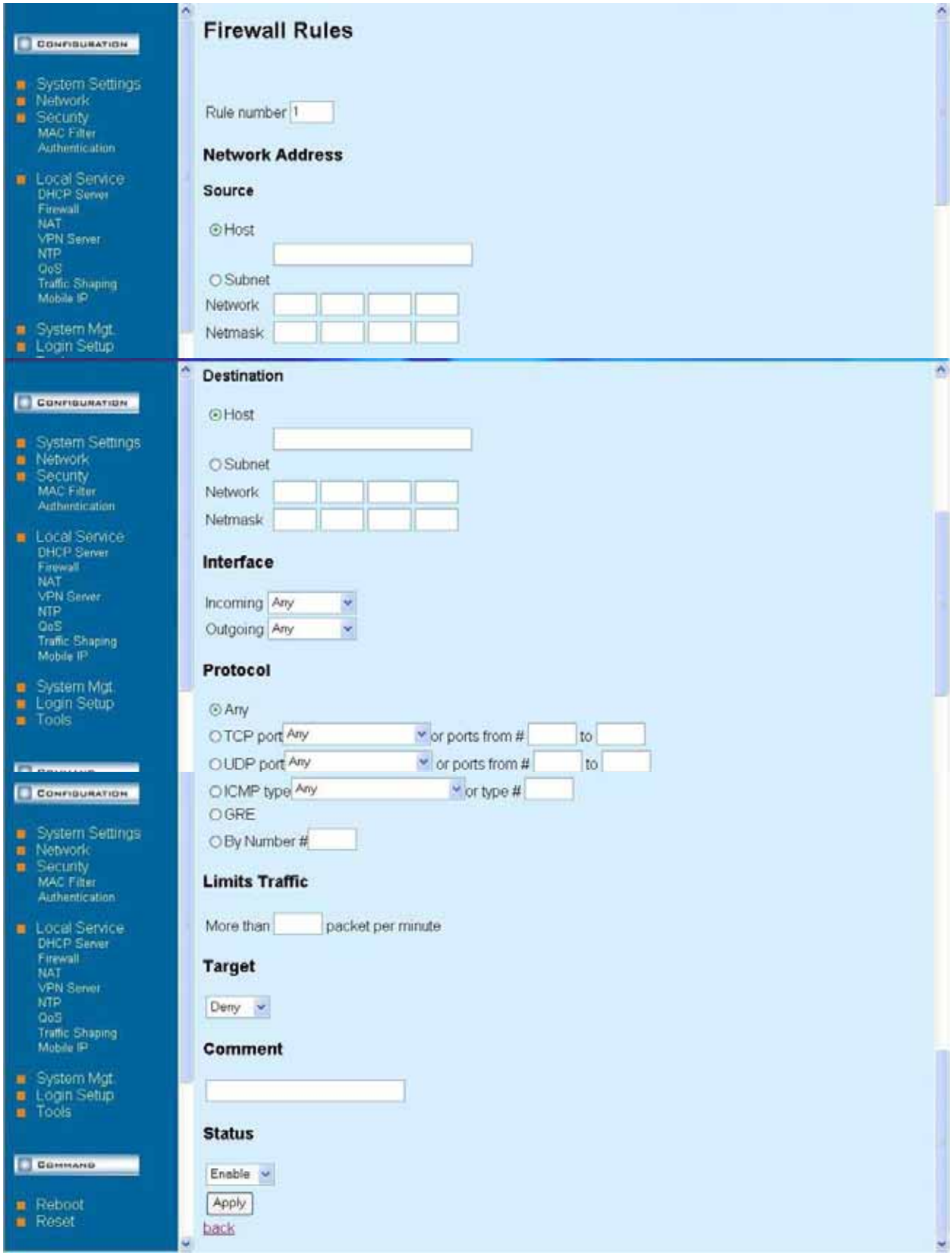
        - Fix the Hardware address to a fixed IP
    - To this IP
        - Fix the Hardware address to this IP
    - Comment
        - Optional comments for this entry
    - Status
        - Enable or disable this entry

2.3.10 Configuration->Local Services->Firewall

To safeguard MESH AP from any intruders, MESH AP features a customizable firewall. The firewall stops and blocks any unauthorized user access from the WAN port. It used to control both incoming and outgoing data. To customize the firewall, the rules need to be specified. MESH AP monitors the IP datagram that travel in and out, analyzes the packet based on the firewall rules, and decides whether to accept or deny that packet. Firewall rules apply to both wired and wireless LAN network interfaces.

Firewall Parameters:

- Enable Firewall
    - To enable or disable the firewall
- Default Policy
    - Set the default policy for the firewall rule
    - Select Option: Accept or Deny
    - Default value: Accept
- Existing Rules
    - Display the current firewall rules
- Click “Add” button to add new rules.
- Click “Edit” button to edit the selected rule.



Firewall Rules Parameters:

- Rule Number
  - To specify the rule number of this entry
- Source
  - Host

        - To specify the hostname in FQDN form or IP address as the source address
    - Subnet
        - Network
            - To specify the network IP address as the source address
            - Example: 192.168.5.0
        - Netmask
            - To specify the network mask
            - Example: 255.255.255.0
- Destination
    - Host
        - To specify the hostname in FQDN form or IP address as the source address
    - Subnet
        - Network
            - To specify the network IP address as the destination address
            - Example: 192.168.1.5
        - Netmask
            - To specify the network mask
            - Example: 255.255.255.255
- Source Interface
    - To specify the interface as the source interface
    - Option: Any, WLAN/LAN, WAN, LINK
- Destination Interface
    - To specify the interface as the destination interface
    - Option: Any, WLAN/LAN, WAN , LINK
- Protocol
    - To specify the protocol of the rule to check
    - Option
        - Any
            - Rules apply to any protocol
        - TCP
            - Rules apply to TCP protocol
            - Specify an unique port or a range of port numbers
        - UDP
            - Rules apply to UDP protocol
            - Specify an unique port or a range of port numbers
        - ICMP
            - Rules apply to ICMP protocol
            - Specify the ICMP type
        - GRE
            - Rules apply to GRE protocol
        - By number #

          Rules apply to specified port number such as ICQ defined port
- Limits traffic
    - Matching rule to limit the traffic for certain application
    - More than #packet per minute
    - Example: Rule: 5 packet per minute, and allow FTP packets. This means this rule is applied only when the number 6 FTP packet is received for that minute
- Target
    - To set the policy to the target rule
    - Option: Deny, Accept, Free
        - Deny: To reject the packet that match the rule

        - Accept: To accept the packet that match the rule
        - Free: To provide the free access to that particular rule
- Comments
    - To specify the comments of the rule
- Status
    - Enable or disable this rule

2.3.11 Configuration->Local Services->NAT

NAT (Network Address Translation) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. Typically, a company maps its local inside network addresses to one or more global outside IP addresses and unmaps the global IP addresses on incoming packets back into local IP addresses. This helps ensure security since each outgoing or incoming request must go through a translation process that also offers the opportunity to qualify or authenticate the request or match it to a previous request. NAT also conserves on the number of global IP addresses that a company needs and it lets the company use a single IP address in its communication with the world.

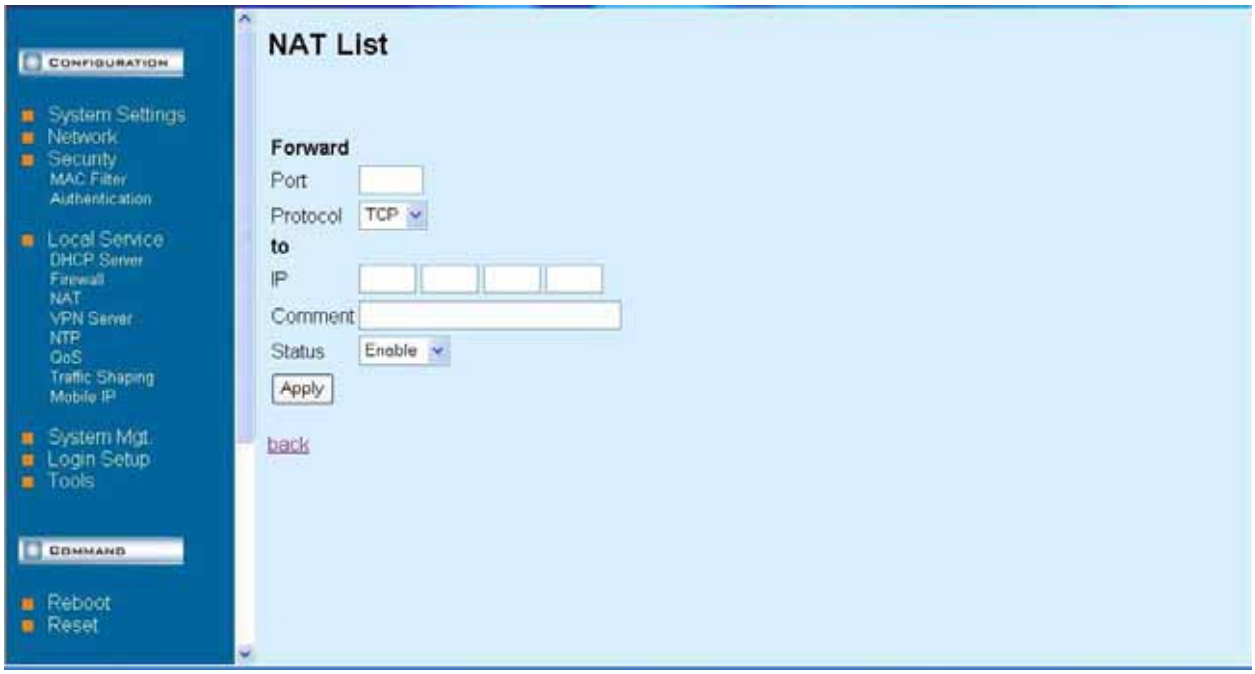
NAT is included as part of a router and is often part of a corporate firewall. Network administrators create a NAT table that does the global-to-local and local-to-global IP address mapping. NAT can also be used in conjunction with *policy routing*. NAT can be statically defined or it can be set up to dynamically translate from and to a pool of IP addresses. MESH AP of NAT lets an administrator create tables that map:

- A local IP address to one global IP address statically
- A local IP address to any of a rotating pool of global IP addresses that a company may have
- A local IP address plus a particular TCP port to a global IP address or one in a pool of them
- A global IP address to any of a pool of local IP addresses on a round-robin basis

NAT Parameters:

- Enable NAT
  - To enable or disable the NAT service
- NAT Table
  - A list of existing NAT rules
- Click “Apply” to save configuration changed
- Click “Add” to add new entry to the NAT table

- Click “Edit” to edit selected entry

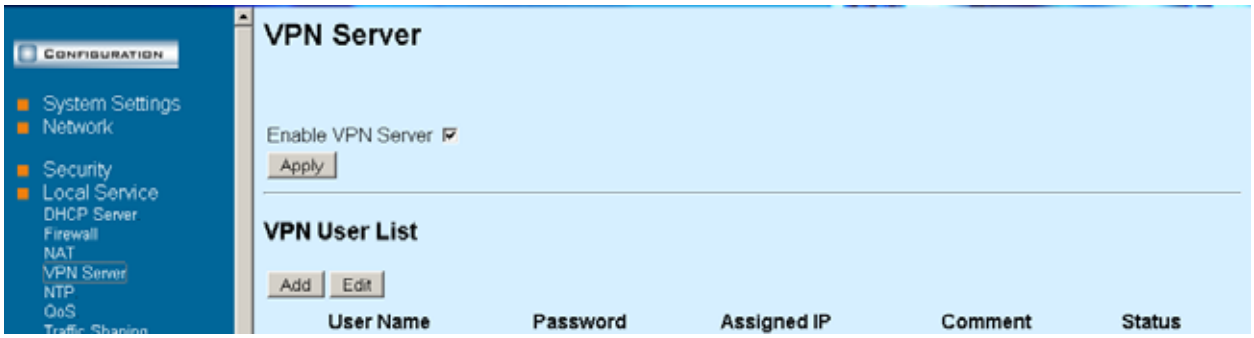


NAT List Parameters:

- Port
  - To specify the port of the entry
  - Example: 23 (telnet)
- Protocol
  - To specify the protocol of the entry
  - Option: TCP , UDP
- IP
  - To specify the IP of the entry
  - Example: 192.168.1.25
- Comment
  - To specify optional comment for this entry
- Status
  - Enable or disable this entry
- Example: Forward port 23 telnet traffic to host 192.168.1.25 by entering 23 to port, tcp protocol, and 192.168.1.25 to the IP
- Click “Apply” to save the configuration changed.

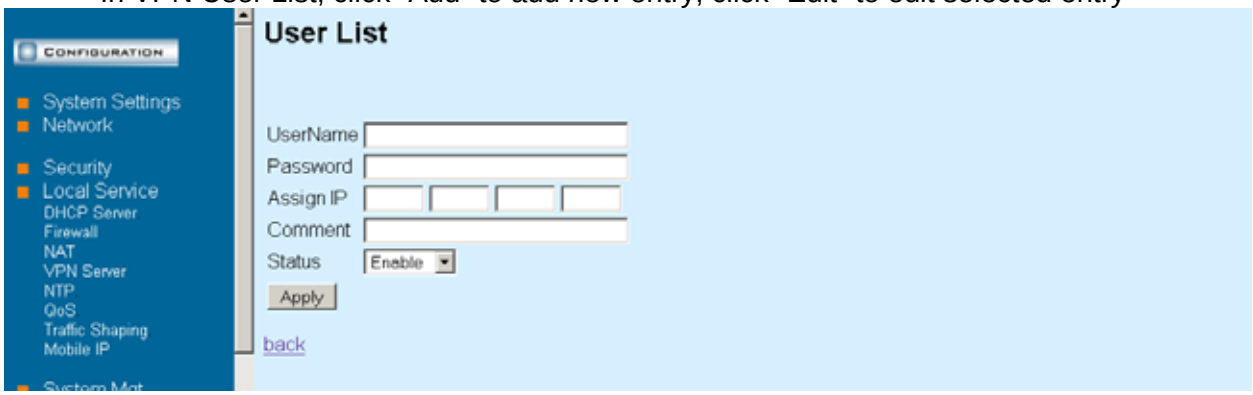
2.3.12 Configuration->Local Services->VPN Server

This submenu defines the configurations of built-in virtual private network (VPN) connection from a remote network. The traffic in the VPN tunnels is encrypted and protected against eavesdropping. Authentication and management traffic can be protected through the PPTP tunnel.



VPN Server Parameters:

- Enable VPN Server
  - To enable or disable the VPN Server service
  - Example: enabled
- Click “Apply” to save configuration changed
- In VPN User List, click “Add” to add new entry, click “Edit” to edit selected entry



- User List Parameters
  - Username
    - To specify the username of a VPN user
  - Password
    - To specify the password of the VPN user
  - Assign IP
    - To specify the IP assigned to this VPN user
  - Comment
    - To specify optional comments on this entry
  - Status
    - Enable or disable this entry

2.3.13 Configuration->Local Services->NTP-Client

Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock times in a network of computers. Developed by David Mills at the University of Delaware, NTP is now an Internet standard. In common with similar protocols, NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes to a fraction of a millisecond.

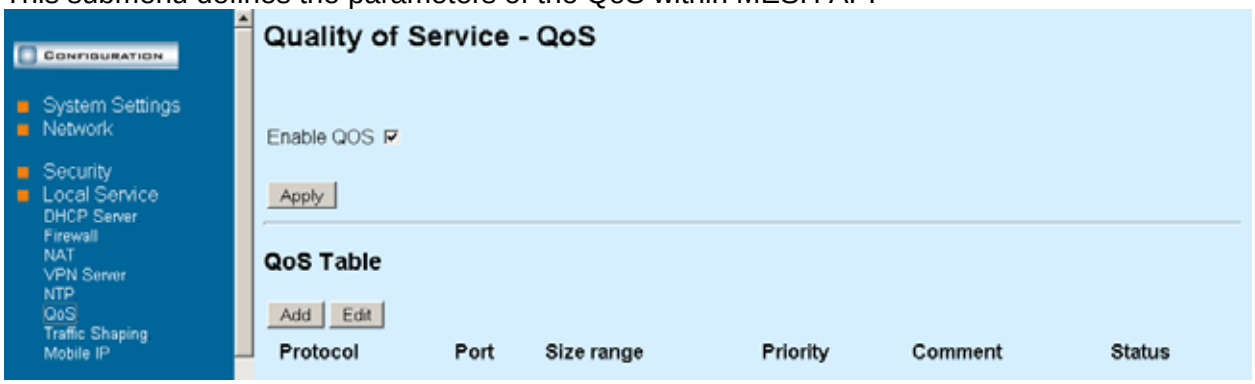
The term NTP applies to both the protocol and the client/server programs that run on computers. MESH AP acts as the NTP client that initiates a time request exchange with the time server. As a result of this exchange, the client is able to calculate the link delay, its local offset, and adjust its local clock to match the clock at the server's computer.

NTP Client Parameters:

- Enable NTP
  - To enable or disable the NTP client service
- Server 1
  - To specify the IP of the NTP server
  - Example: pool.ntp.org
- Server 2
  - To specify the IP of the NTP server
- Server 3
  - To speciry the IP of the NTP server
- Timezone
  - To specify the timezone
- Click “Apply” to save the configuration changed

2.3.14 Configuration->Local Services->QoS

This submenu defines the parameters of the QoS within MESH AP.



QOS parameters:

- Enable QOS
  - To enable or disable the QOS setting
- Click “Add” to add new entry to the QoS table
- Click “Edit” to edit the selected entry

- QoS list parameters:
  - Protocol
    - To specify the protocol of this entry
  - Port
    - To specify the port of this entry
  - Packet size
    - To specify the size of the packet of this entry
  - Priority
    - To prioritize this entry
  - Comment
    - To specify optional comment on this entry
  - Status
    - Enable or disable this entry

2.3.15 Configuration->Local Services->Traffic Shaping

This submenu defines the parameters of the traffic shaping within MESH AP. Traffic is very important to limit certain user not to use more than assigned bandwidth.

QoS Parameters:

- Enable QoS
  - To enable or disable the QoS service
- Default Upload
  - To specify the default upload bandwidth in kbps per user basis
  - Example: 256
- Default Download
  - To specify the default download bandwidth in kbps per user basis
  - Example: 256
- Click “Apply” to save configuration changed.

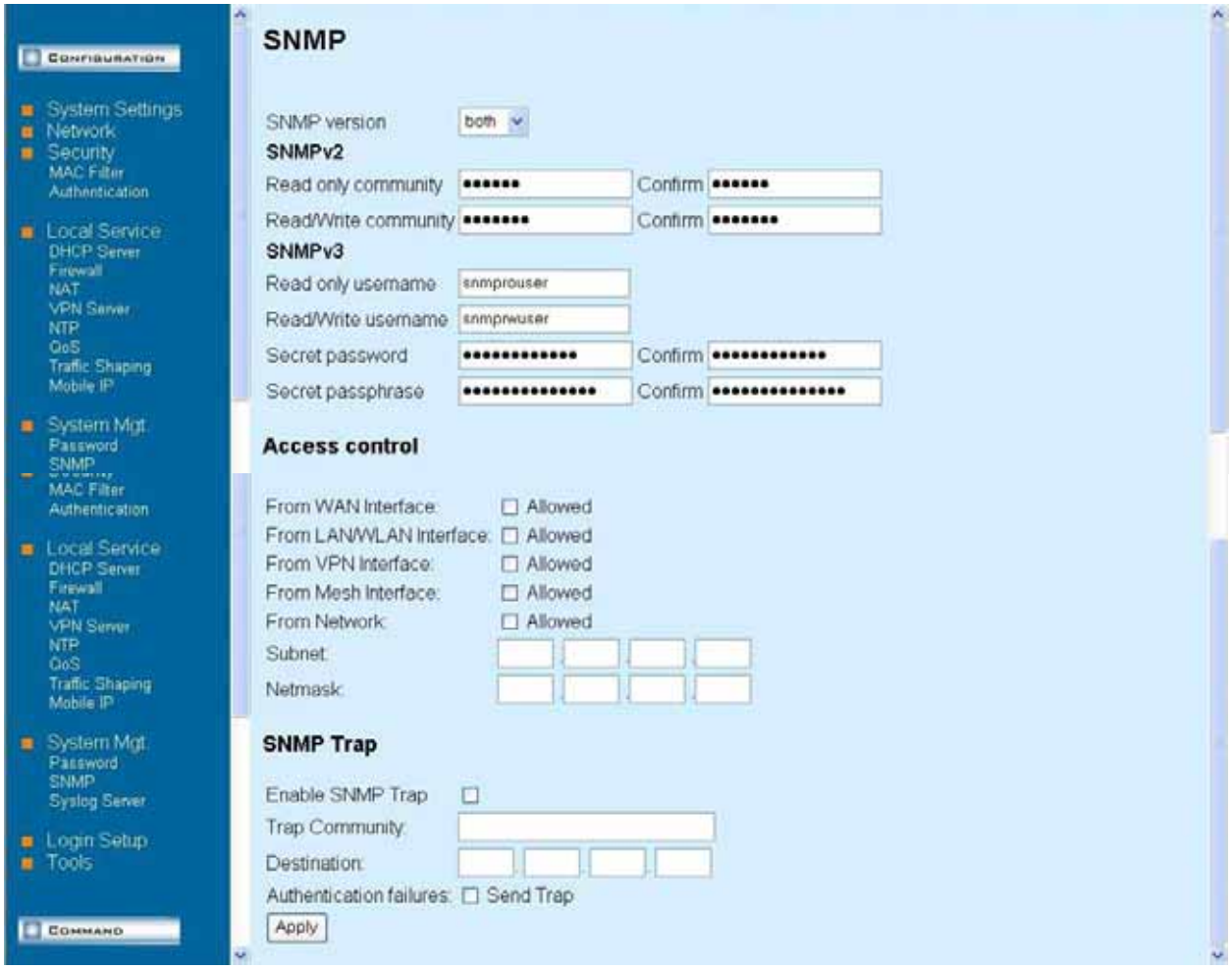
2.3.16 Configuration->System Management->Password

This submenu allows user to change the administrator login password.

Password Parameters:

- New Password
  - To specify the new web-based configuration password
- New Password
  - To specify the entered new password again for verification purpose
- Click “Apply” to save configuration changed.

2.3.17 Configuration->System Management->SNMP



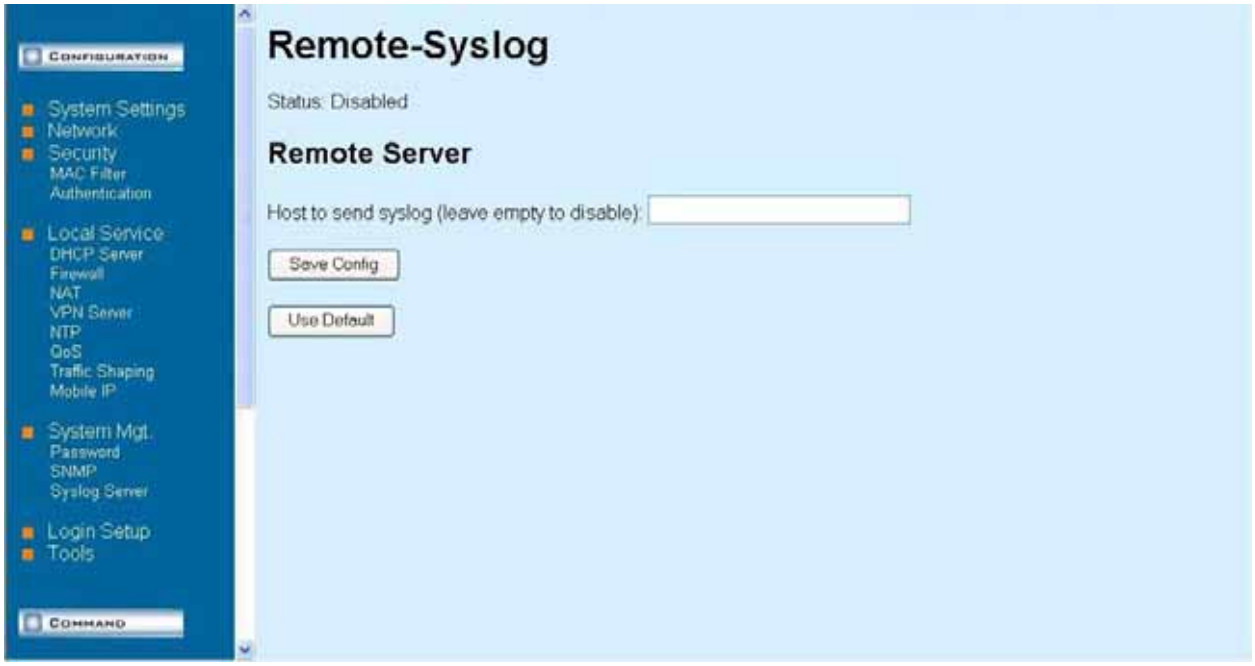
SNMP Password Parameters:

- SNMP Version
  - To specify the version of the SNMP
- SNMP v2 Read Password
  - To specify the SNMP-v2 read password
- SNMP v2 Read/Write Password
  - To specify the SNMP-v2 read/write password
- SNMP v3 Read Password
  - To specify the SNMP-v3 read password
- SNMP v3 Read/Write Password
  - To specify the SNMP-v3 read/write password
- SNMP v3 Secret Password
  - To specify the SNMP-v3 secret password
- SNMP v3 Secret Passphrase
  - To specify the SNMP-v3 secret passphrase
- Access control
  - From WAN
    - To allow access from WAN interface
  - From LAN/WLAN
    - To allow access from LAN/WLAN interface
  - From VPN
    - To allow access from VPN interface

    - From Mesh
        - To allow access from mesh network
- SNMP Trap
    - Enable SNMP Trap
        - Enable or disable the SNMP trap
    - Trap Community
        - To specify community for the SNMP trap
    - Destination
        - To specify the destination of the trap
    - Authentication failures
        - Enable or disable if authentication failures
- Click “Apply” to save configuration changed

2.3.18 Configuration->System Management->Remote-Syslog

The capability of remote logging is critical to the functionality of the MESH AP. With remote logging, remote syslog server can monitor all traffic coming through the firewall, any system changes, and even system information from the MESH AP. The remote system logger review the log files from the MESH AP and decide what to do when specific events occur.

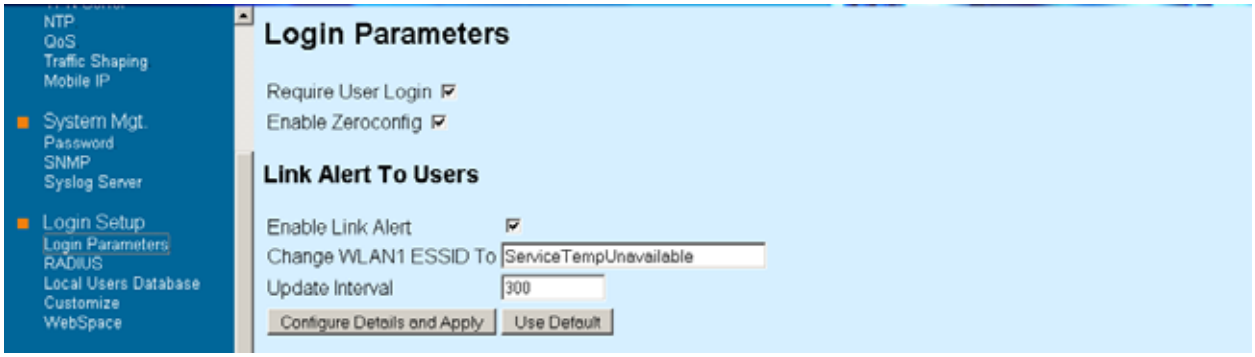


Remote-Syslog Parameters:

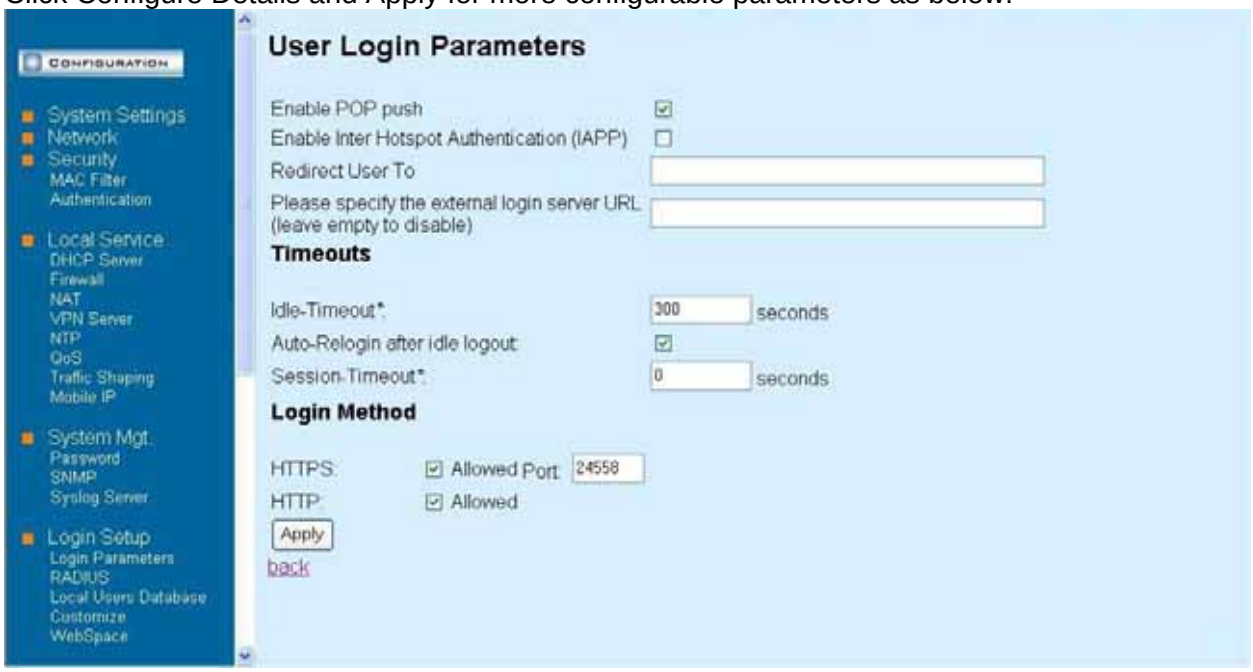
- Remote Server
    - To specify the IP address of the remote syslog server.
- Click “Save Config” to save configuration changed.

2.3.19 Configuration->Login Setup->Login Parameters

This submenu contains the login parameters to the external RADIUS server connection.



Click Configure Details and Apply for more configurable parameters as below:



Login Parameters:

- Require User Login
  - To enable or disable the MESH AP Login service
- External Login Server
  - To specify the URL for the external login server
  - Leave empty to disable this feature
- Idle-Timeouts
  - To specify idle-timeouts in seconds
  - Value entered will be override by RADIUS server
  - Default value: 5 minutes
- Auto-Relogin after idle logout
  - Click to enable the auto-relogin after idle timeout
- Session-Timeout
  - To specify session-timeout in seconds
  - Value entered will be override by RADIUS server
  - Default value: 0 minutes
- HTTPS allowed
  - To enable or disable the login through https
- HTTP allowed
  - To enable or disable the login through http
- Click “Apply” to save configuration changed
- Click “Use Default” to use the default value

2.3.19.1 Using the External Login Server

MESH AP provides an option that allows administrator to redirect users to a remote server to log in to the public access interface instead of using the internal login page.

The advantages of using the external login server are listed as follow:

- The login page is completely customizable and centralized located at the web server.
- Users can login to the public access interface without exposing their web browsers to the SSL certificate on the MESH AP. Warning messages caused by having an SSL certificate on the MESH AP that is not signed by a well-known certificate authority is eliminated.
- Only a single SSL certificate signed by a well-known certificate authority is required for the remote web server. There is no need to obtain the SSL certificate for every MESH AP.

External Login could be used, for example to deploy a centralized login portal. Following diagram shows the sequence of the login process when a client start access internet using MESH AP Access Point.

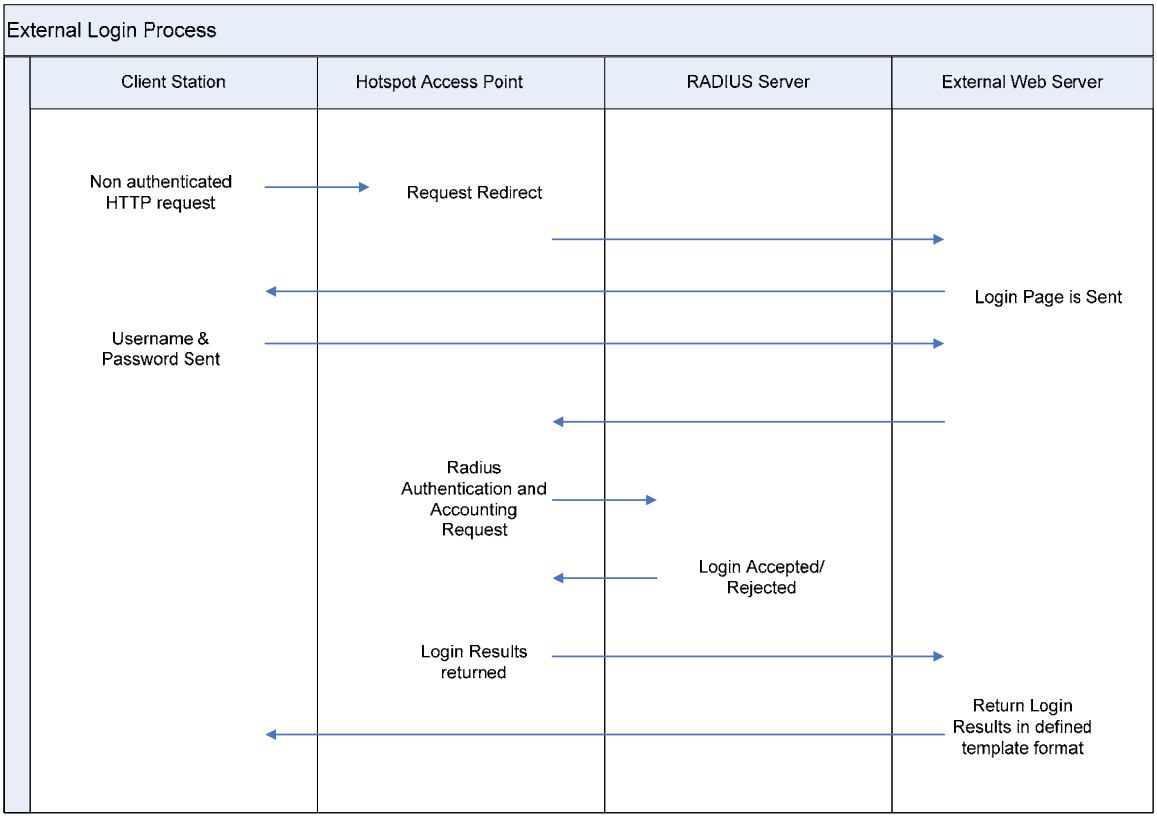


Figure. External Login Process

2.3.19.1.1 Configuring the MESH AP

Login to the access point configurations, under Login Setup->User Login Parameters, enter the External Login URL (e.g. https://www.server.com/Login.php?client=##CLIENT_IP##). There are several macros available in order to retrieve information from the access point.

Macro	Description
##CLIENT_IP##	The IP address of the login client
##REQUESTED_URL##	Original URL on which the client is requesting.

##GATEWAY_LOGIN##	The Access Point's external login gateway. (https://<accesspoint-domain>:<https_port>/X_Login.cgi) Where <accesspoint-domain> is the Common Name (CN) found in the Webserver Certificates. <https_port> is the configured Secure login port
##EXT_IP##	Return the WAN IP address of the access point
##NAS_ID##	Return the NAS Identifier of the access point
##DOMAIN##	Return the hostname (CN in the certificates)
##PORT_HTTPS##	Return the secure login port of the access point

Table – Defined Macros in the external login URL

Note that, the external server hostname must be able to resolve by the Access Point for proper Access Control Setup. (This could be verified using the Tools->Ping page in the web based configurations page).

Access Control to the external server is automatically done during startup or after configured the new server address. Thus, **if** the external server is using dynamic IP address, the Access Control will become invalid after the address has changed.

2.3.19.1.2 Gateway Login URL

This is the gateway between the external server and the access point's radius client. External server will have to send back the

- USERNAME,
- PASSWORD,
- CLIENT_IP

information to the access point. All information should be encoded according to the RFC 1738 specification. E.g. for the username 'Donald Duck', the POST should contain USERNAME=Donald%20Duck.

2.3.19.1.3 Gateway Logout URL

External server could, forcing a logged-in station to logout using the logout URL.
https://<accesspoint-domain>:<https_port>/X_Logout.cgi?CLIENT_IP=<client ip address>

2.3.19.1.4 Login Reply

After processing the authentication request, the Access Point will reply the External Server with the following contents:

2.3.19.1.4.1 Login Success

```
<HTML>
<!--
<?xml version="1.0" encoding="UTF-8"?>
<WISPAccessGatewayParam
```

```
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://www.acmeWisp.com/WISPAccessGatewayParam.xsd">
<AuthenticationReply>
<MessageType>120</MessageType>
<ResponseCode>50</ResponseCode>
<ReplyMessage>" radius reply message"</ReplyMessage>
</AuthenticationReply>
</WISPAccessGatewayParam>
-->
<!--
<LOGIN>SUCCESS</LOGIN>
<REQUESTED_URL>Original Requested URL </REQUESTED_URL>
<SERVER_NAME>Access Point Hostname </SERVER_NAME>
<INTERNAL_WEBSPACE_URL>Access Point Internal Webspace URL </INTERNAL_WEBSPACE_URL>
<USER_STATUS_URL>Access Point Internal url to check user status </USER_STATUS_URL>
<USER_IP>client IP address </USER_IP>
<USER_MAC>client machine MAC address </USER_MAC>
<USER_LOGINNAME>login name </USER_LOGINNAME>
<USER_AUTH_MODE>authentication mode </USER_AUTH_MODE>
<USER_AUTH_MSG>radius reply message </USER_AUTH_MSG>
<USER_IDLE_TIMEOUT>user idle timeout </USER_IDLE_TIMEOUT>
<USER_SESSION_TIMEOUT>user session timeout</USER_SESSION_TIMEOUT>
<USER_CUSTOM>radius custom reply attributes</USER_CUSTOM>
<LOGIN_DNS_KEYWORDS>dns shortcut to the access point logout url</LOGIN_DNS_KEYWORDS>
-->
<body>LOGIN SUCCESS</body>
</html>
```

2.3.19.1.4.2 Already Logged In

```
<HTML>
<!--
<?xml version="1.0" encoding="UTF-8"?>
<WISPAccessGatewayParam
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://www.acmeWisp.com/WISPAccessGatewayParam.xsd">
<AuthenticationReply>
<MessageType>120</MessageType>
<ResponseCode>100</ResponseCode>
<ReplyMessage>" radius reply message"</ReplyMessage>
</AuthenticationReply>
</WISPAccessGatewayParam>
-->
<!--
<LOGIN>ERROR</LOGIN>
<USER_STATUS_URL>Access Point Internal url to check user status </USER_STATUS_URL>
<USER_IP>client IP address </USER_IP>
<USER_MAC>client machine MAC address </USER_MAC>
<USER_LOGINNAME>login name </USER_LOGINNAME>
<USER_AUTH_MODE>authentication mode </USER_AUTH_MODE>
<USER_AUTH_MSG>radius reply message </USER_AUTH_MSG>
<USER_IDLE_TIMEOUT>user idle timeout </USER_IDLE_TIMEOUT>
<USER_SESSION_TIMEOUT>user session timeout</USER_SESSION_TIMEOUT>
<USER_CUSTOM>radius custom reply attributes</USER_CUSTOM>
<LOGIN_DNS_KEYWORDS>dns shortcut to the access point logout url</LOGIN_DNS_KEYWORDS>
-->
<body>ALREADY LOGGED IN</body>
</html>
```

2.3.19.1.4.3 Login Denied

```
<HTML>
<!--
<?xml version="1.0" encoding="UTF-8"?>
<WISPAccessGatewayParam
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:noNamespaceSchemaLocation="http://www.acmeWisp.com/WISPAccessGatewayParam.xsd">
<AuthenticationReply>
<MessageType>120</MessageType>
<ResponseCode>100</ResponseCode>
<ReplyMessage>" radius reply message"</ReplyMessage>
</AuthenticationReply>
</WISPAccessGatewayParam>
-->
<!--
<LOGIN>ERROR</LOGIN>
<REQUESTED_URL> Original Requested URL </REQUESTED_URL>
<SERVER_NAME> Access Point Hostname </SERVER_NAME>
<USER_LOGINNAME> login name </USER_LOGINNAME>
<USER_AUTH_MSG> radius reply message </USER_AUTH_MSG>
-->
<body>LOGIN DENIED</body>

</html>
```

2.3.19.1.5 Certificates and hostname

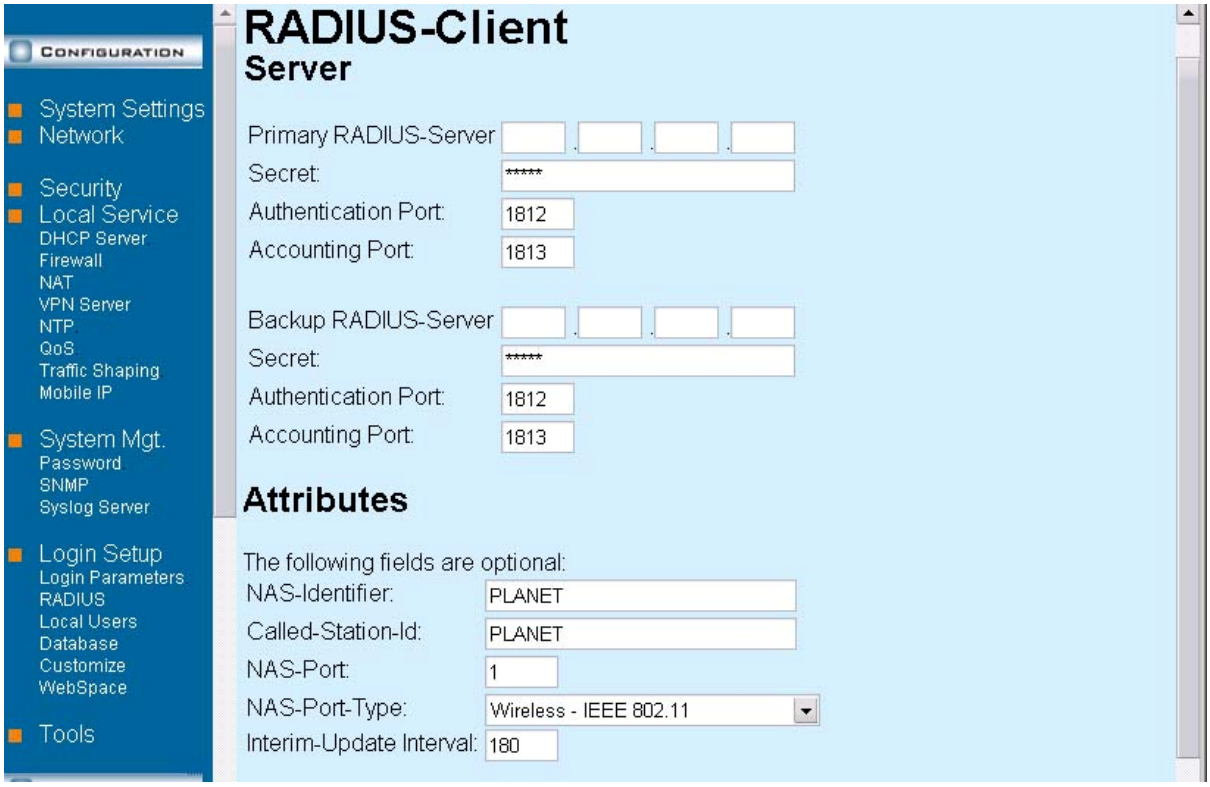
The Access Point will use the subject CN field in the installed certificates as its default hostname (provided the CN field contains a valid hostname, only [.-a-zA-Z] character is allowed).

AP returns the hostname as GATEWAY_LOGIN URL by default. External server could use the ##EXT_IP## or using the REMOTE_ADDR variable from the HTTP server, to obtain the AP IP address, if the hostname is not a known to the server.

2.3.20 Configuration->Login Setup->Radius

Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point. Having a central service also means that it's easier to track usage for billing and for keeping network statistics. Created by Livingston (now owned by Lucent), RADIUS is a de facto industry standard used by a number of network product companies and is a proposed IETF standard.

This submenu contains all options to define the settings that MESH AP need to communicate to the external RADIUS server. It contains login, RADIUS, and local users. The following sections explain the configuration parameters in detail.



Radius-Client Parameters:

- Server
  - Primary RADIUS-Server
    - To specify the IP address of the primary RADIUS server
    - Example: 192.168.1.2
  - Secret
    - To specify the login password of the primary RADIUS server
    - Example: secretpassword
  - Authentication Port
    - To specify the authentication port for the primary RADIUS server
    - Default value: 1812
  - Accounting Port
    - To specify the accounting port for the primary RADIUS server
    - Default value: 1813
  - Backup RADIUS-Server
    - To specify the IP address of the secondary RADIUS server
  - Secret
    - To specify the login password of the secondary RADIUS server
  - Authentication Port
    - To specify the authentication port for the secondary RADIUS server
  - Accounting Port
    - To specify the accounting port for the secondary RADIUS server

- Attributes.
  - NAS-Identifier
    - To specify the Network Access Server (NAS) identifier for the MESH AP. This ID attribute is included in all packets that send to RADIUS server.
  - Called-Station-Id
    - To specify the MESH AP RADIUS client ID
  - NAS-Port

  - To specify the NAS port number for authentication
- NAS-Port-Type
  - To specify the type of NAS port
- Interim-Update interval
  - To specify the interval of updates to RADIUS server

2.3.21 Configuration->Login Setup->Local Users Database

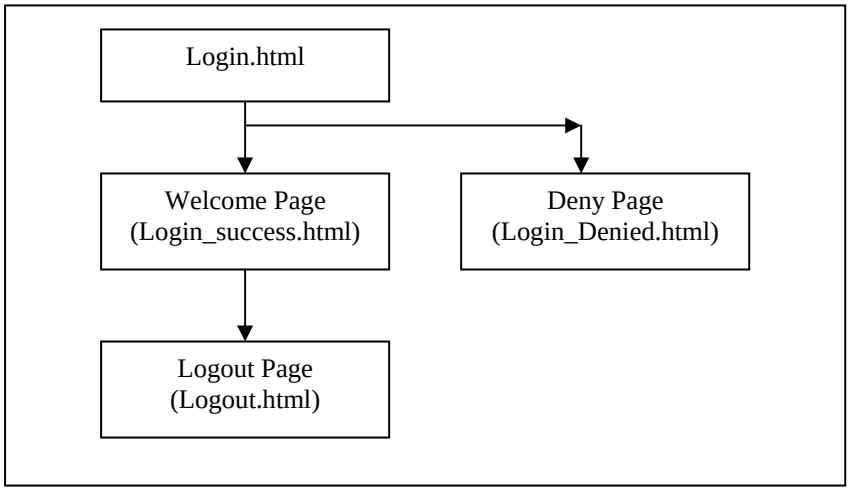
Local Users Database

- List of Users
  - To display current local users
  - Click “Delete” to remove a local account
  - Click “Change Password” to change the password of that account
- Add new User

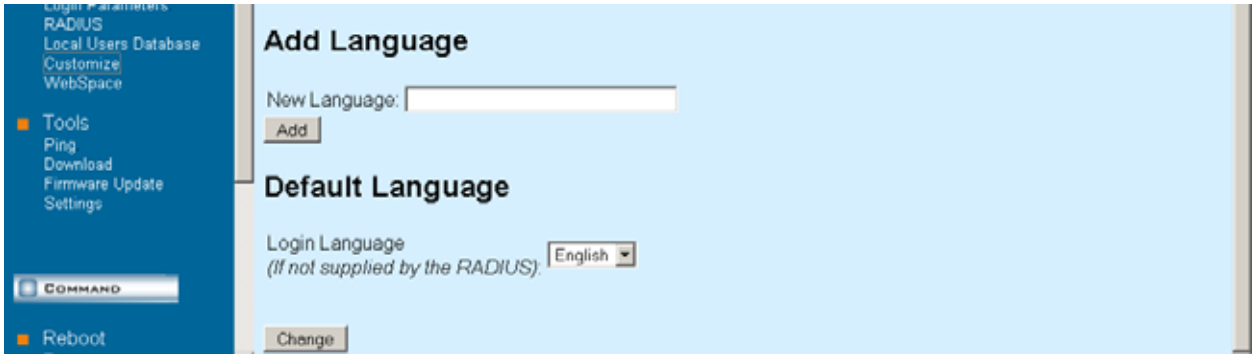
- Username
  - To specify the new local user login name
- Password
  - To specify the new local user login password
- Password(repeat)
  - To specify the new local user login password again for verification
- Click “Add new User” to add the new local user

2.3.22 Configuration->Login Setup->Customize

The login page can be customized to serve the administrator requirements. The administrator can upload his or her own web design to the MESH AP. Figure below shows the login sequence. After a successful login, the user is identified and his or her preference language is known if the RADIUS server has sent that option. Therefore, the welcome and logout page can be adjusted according to the language.



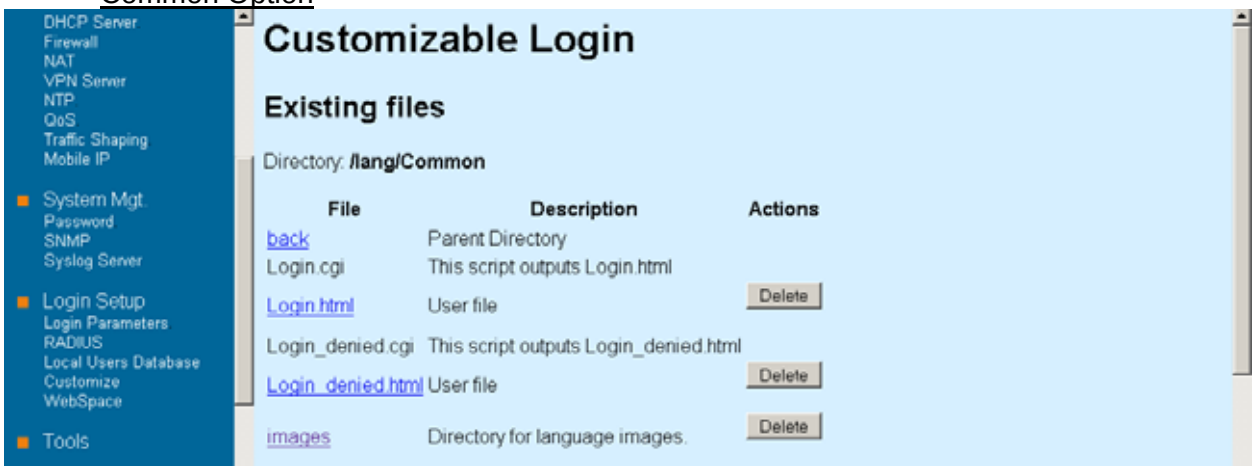
This submenu contains the configurations for administrator to customize his or her login, welcome, deny, and logout pages. MESH AP uses English as default preference language. Administrator can also customize his or her preference language.

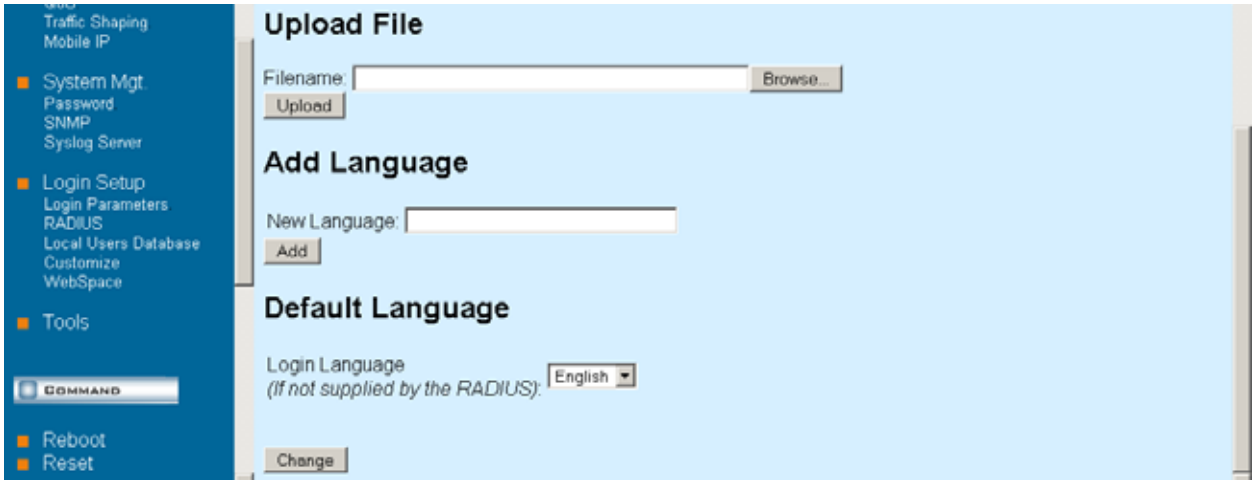


Customizable login Parameters

- Existing Files
  - To display the available current language and customized pages of MESH AP
  - Common
    - Contains the customized language independent web page such as login.html & login_denied.html
    - Click the link to access the common folder
  - English
    - Contain the language dependent webpage such as login_success.html & logout.html
    - Click the link to access the ‘language’ folder
- Upload Files
  - To upload the customized web pages to the MESH AP
- Add Language
  - To add in a new language
  - Enter the language name and click the ‘Add’ button.
- Default Language
  - The default language is preset to “English”

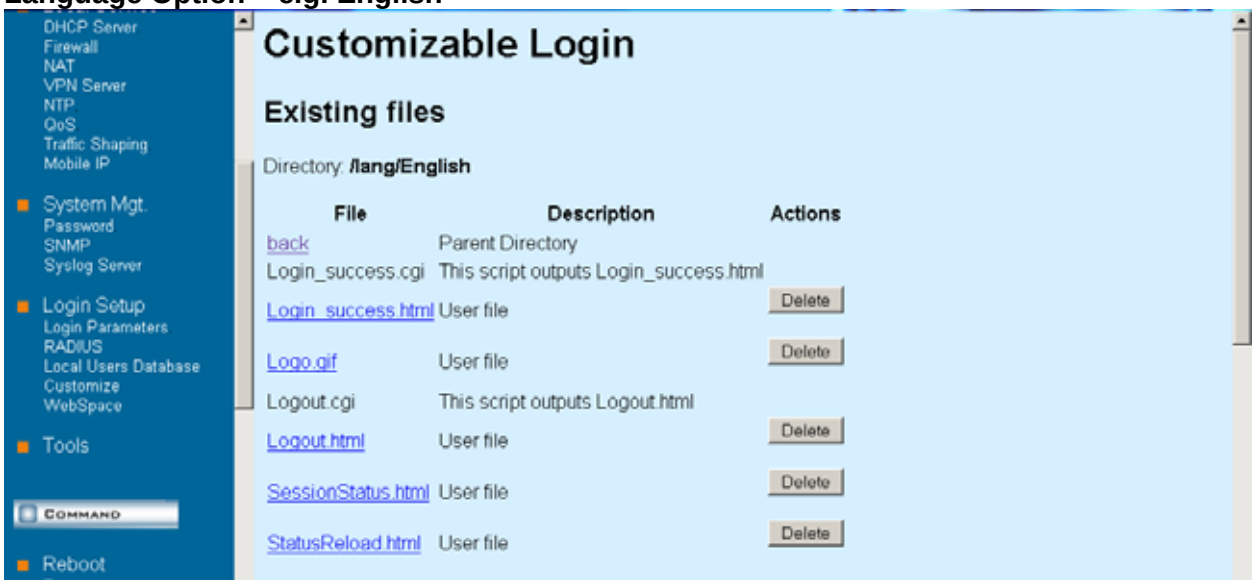
Common Option

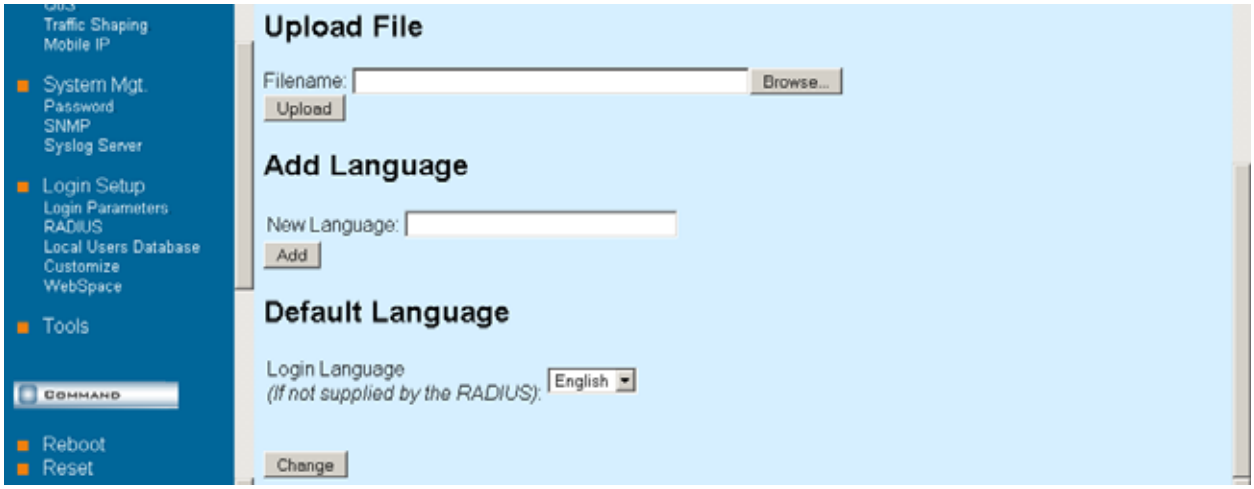




- Existing files
  - Show the existing common folder web pages
  - To upload a new customized page, click 'Delete' button to remove the existing customized page and upload the new file.
- Click 'back' to link back to customizable login main page
- Upload Files
  - To upload the customized web pages to the MESH AP
- Add Language
  - To add in a new language
  - Enter the language name and click the 'Add' button.
- Default Language
  - The default language is preset to "English"

Language Option – e.g. English





- Language Common Folder Parameters
  - Existing files
    - Show the existing common folder web pages
    - To upload a new customized page, click 'Delete' button to remove the existing customized page and upload the new file.
  - Click 'back' to link back to customizable login main page
  - Upload Files
    - To upload the customized web pages to the MESH AP
  - Add Language
    - To add in a new language
    - Enter the language name and click the 'Add' button.
  - Default Language
    - The default language is preset to "English"

Description of RADIUS-Client

Several parameters are transmitted from and to the RADIUS-Server, to allow centralized logging and configuration on a per-user base. The following data is exchanged with the RADIUS. Attributes starting with PLANET are vendor attributes with the vendor ID 22222 (ID will change).

RADIUS-Attribute	Description
User-Name	Login name
User-Password	Login Password

Table 1 Attributes send to the RADIUS during Login (authentication)

RADIUS-Attribute	Description
Reply-Message	Message to display to the user. Can be accessed by the login macro ##USER_AUTH_MSG##.
Idle-Timeout	Idle timeout in seconds
Session-Timeout	Session timeout in seconds
login-language	Preferred language of the user. Attribute type 1. Accessible by the macro ##USER_LANGUAGE##. The string can contain only the characters [a-zA-Z0-9].

RADIUS-Attribute	Description
login-url	The URL, the user should be redirected after successful login. Attribute type 2. Accessible by the macro ##USER_STARTPAGE##.
login-custom	Full freely cusumizable information, which can be send to by the RADIUS. An example for the usage can be to provide account information, local news, etc. It is also possible to pass multiple arguments in one string and separate them using Java script. The Attribute type is 200 and it is accessible via the macro ##USER_CUSTOM##.

Table 2 Attributes accepted from the RADIUS during Login (authentication)

RADIUS-Attribute	Description
User-Name	Login name
Acct-Status-Type	Value='Start'. Indicates start of Session to the RADIUS

Table 3 Attributes send to the RADIUS during Login (accounting)

RADIUS-Attribute	Description
<none>	

Table 4 Attributes accepted from the RADIUS during Login (accounting)

RADIUS-Attribute	Description
User-Name	Login name
Acct-Status-Type	Value='Stop'. Indicates stop of session
Acct-Input-Octets	The number of bytes received by the user
Acct-Output-Octets	The number of bytes transmitted by the user
Acct-Input-Packets	The number of packets received by the user
Acct-Output-Packets	The number of packets transmitted by the user
Acct-Session-Time	The time in seconds from logging in until the last time a transmission was detected.

Table 5 Attributes accepted from the RADIUS during Logout (accounting)

- Customizable Login

  The login page can be customized to serve the customers requirements. The customer can upload his own web design to the hotspot AP.

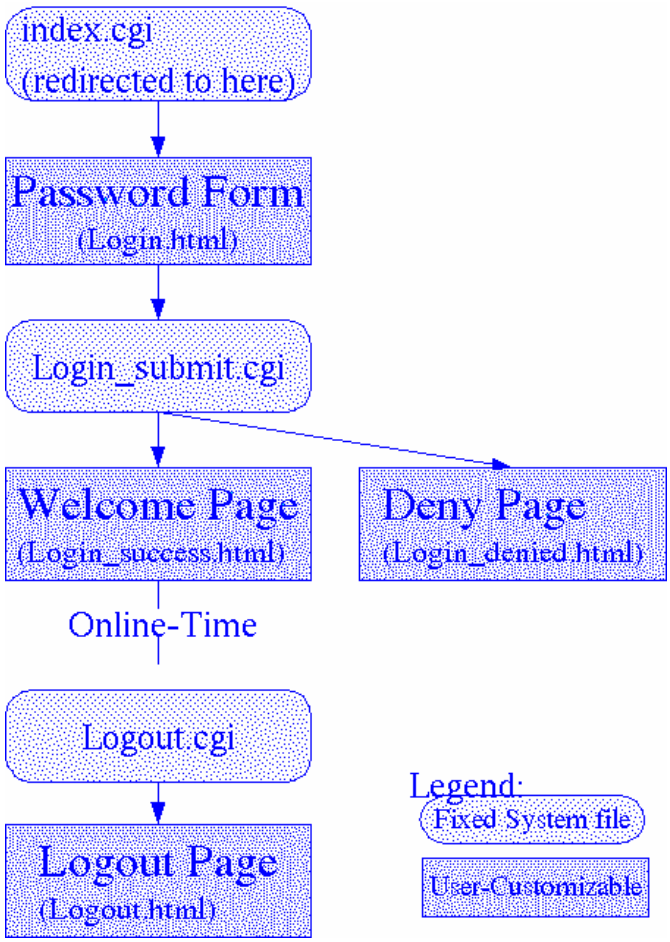


Figure 6.3 - Login Sequence

Figure above shows the login sequence. It consists of system fixed parts, which cannot be modified by the user and parts to be customized. After a successful login, the user is identified and his preferred language is known if it has been sent by the RADIUS server. Therefore the welcome and logout page can be adjusted according to the language.

The files can be uploaded to the hotspot AP and are sharing the flash space with the Web-based configuration. All kinds of files can be uploaded, html, pdf, etc. It just needs to be ensured that the naming of the key files, like Login_success.html remains. In this way, a page can be created on a local PC and afterwards the files can be uploaded, without need to change any link.

The html files are not displayed directly; furthermore they are parsed by a corresponding cgi script in the same directory, which substitutes some macros, which are containing dynamic values like the username and IP address. A sample welcome page looks like this:

```
<HTML>
<BODY>
<H1>Hello ##USER_LOGINNAME##</H1>
</BODY>
</HTML>
```

The following macros can be used:

Macro	Description
##SERVER_NAME##	IP address of the server.
##REQUESTED_URL##	The url, the user requested, before we redirected the request to our login server.

Table 6 Macros for Login.html

Macro	Description
##SERVER_NAME##	IP address of the server.
##REQUESTED_URL##	The url, the user requested, before we redirected the request to our login server.

Table 7 Macros for Login_denied.html

Macro	Description
##SERVER_NAME##	IP address of the server.
##REQUESTED_URL##	The url, the user requested, before we redirected the request to our login server.
##USER_AUTH_MSG##	Reply-Message attribute of the RADIUS server, or english default values if not set. See table 2.
##USER_STATUS_URL##	URL of the status page. This URL should be shown in a seperate window.
##INTERNAL_WEBSPACE_URL##	URL of the internal webspace, which is http://##SERVER_NAME##
##USER_IP##	IP address of the User
##USER_MAC##	MAC address of the user
##USER_LOGINNAME##	Loginname of the user
##USER_AUTH_MODE##	Authentication mode which has been used. Can be either 'local' for authentication via local user database, or 'RADIUS' for authentication via RADIUS.
##USER_STARTPAGE##	The startpage which has been assigned by the RADIUS server, using the login-url attribute. See table 2.
##USER_LANGUAGE##	Preferred language of the user as set by the RADIUS attribute login-language. See table 2.

Macro	Description
##USER_IDLE_TIMEOUT##	Idle timeout in seconds as set by the RADIUS attribute Idle-Timeout. See table 2.
##USER_SESSION_TIMEOUT##	Session timeout in seconds as set by the RADIUS attribute Session-Timeout. See table 2.
##USER_CUSTOM##	Full freely user customizable data, which can be set by the RADIUS attribute login-custom. See table 2.

Table 8 Macros for Login_success.html

Macro	Description
##SERVER_NAME##	IP address of the server.
##USER_IP##	IP address of the User
##USER_MAC##	MAC address of the user
##USER_LOGINNAME##	Loginname of the user
##USER_AUTH_MODE##	Authentication mode which has been used. Can be either 'local' for authentication via local user database, or 'RADIUS' for authentication via RADIUS.
##USER_STARTPAGE##	The startpage which has been assigned by the RADIUS server, using the login-url attribute. See table 2.
##USER_LANGUAGE##	Preferred language of the user as set by the RADIUS attribute login-language. See table 2.
##USER_IDLE_TIMEOUT##	Idle timeout in seconds as set by the RADIUS attribute Idle-Timeout. See table 2.
##USER_SESSION_TIMEOUT##	Session timeout in seconds as set by the RADIUS attribute Session-Timeout. See table 2.
##USER_CUSTOM##	Full freely user customizable data, which can be set by the RADIUS attribute login-custom. See table 2.

Table 9 Macros for Logout.html

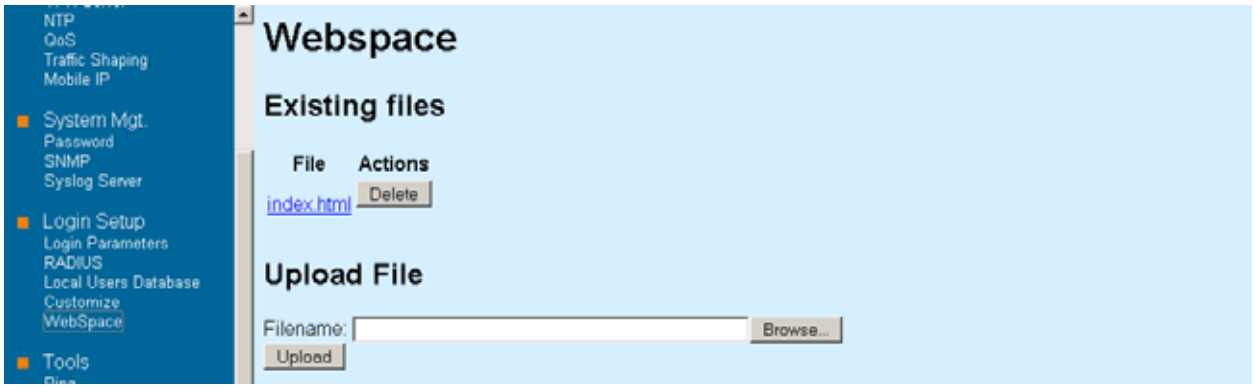
Additionally, each page has the attribute ##HELP##, which enumerates the available attributes.

2.3.23 Configuration->Login Setup->Webspace

Choosing the default page, which is displayed after a successful login, can be useful to provide user some local information, like the menu of a restaurant. At some sites like this restaurant, there can't be assumed to be a network infrastructure, besides the WAN connection. This is maybe also no web server in the Internet to display the menu page.

To serve these customers, it is possible to store a simple page locally in the MESH AP. MESH AP provides up to **1MB** of space for administrator to store some local information.

This submenu allows administrator to manage the local information to be display after successful login of the MESH AP locally.

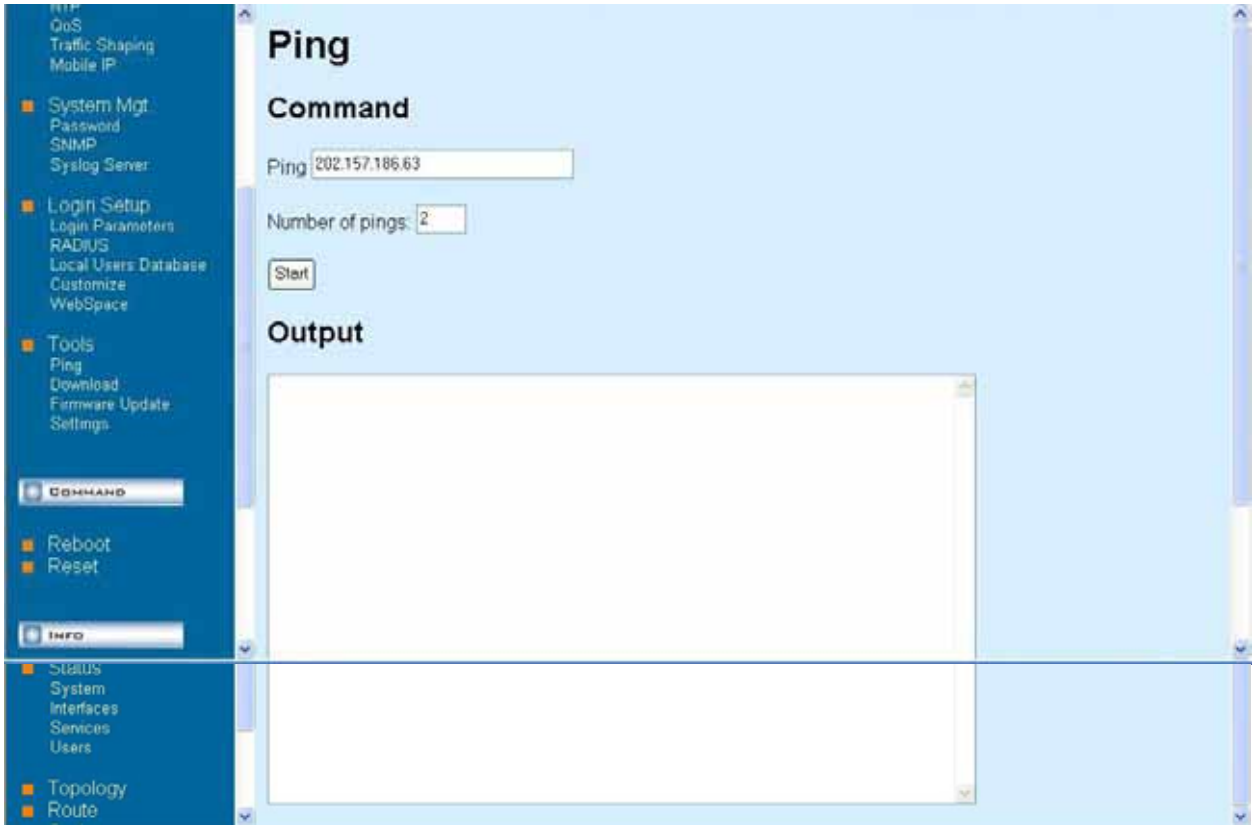


Webspace parameter

- Existing files
  - To display the existing webpages for local information
  - Click "Delete" to remove the selected webpage
- Upload File
  - To upload a new webpage for local information
  - Click "Browse" button to select the file to be uploaded
  - Click "Upload" button to upload the selected file

2.3.24 Configuration->Tools->Ping

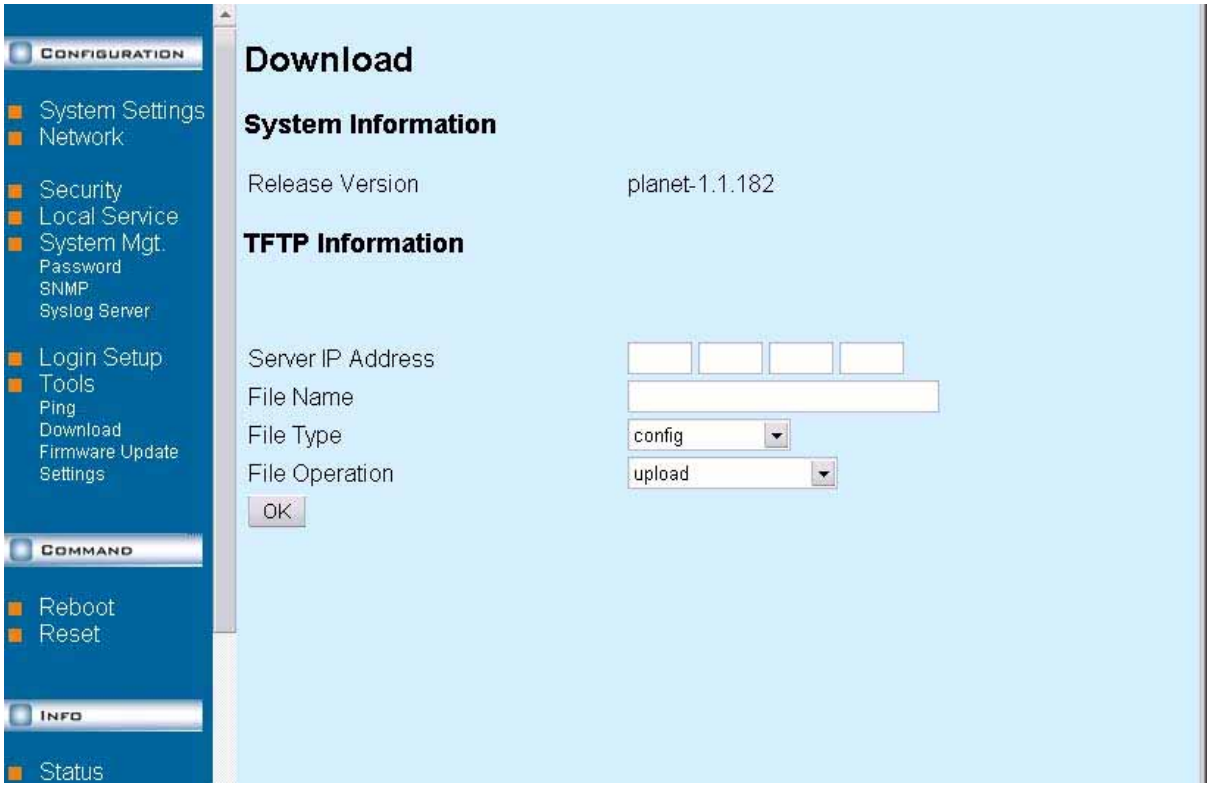
Ping sends ICMP request messages to the network host. The connectivity between the network host and MESH AP is proven working when an ICMP respond message from the network host.



Ping Parameters:

- Ping
  - To specify the host IP address to ping
  - Example: 202.157.186.63
- Number of pings
  - To specify number of count to send the ping command
  - Example: 2
- Click “Start” button to start the Ping command
- Output
  - Display the Ping command result

2.3.25 Configuration->Tools->Download



Download Parameters:

- System Information (Display only)
  - Display the information about the firmware of the system
- Server IP Address
  - To specify the IP address of the TFTP server
  - Example: 192.168.1.91
- File Name
  - To specify the name of the file
  - Example: config
- File Type
  - To specify the file type
  - Option: config, firmware
    - Config- configuration image
    - Firmware- firmware image
- File Operation
  - To specify the operation type
  - Option: upload, download, download and reboot
    - Upload – upload to TFTP server
    - Download – download to MESH AP
    - Download and reboot – reboot after finish download to MESH AP
- Click “Apply” to perform operation

2.3.26 Configuration->Tools->Firmware Update

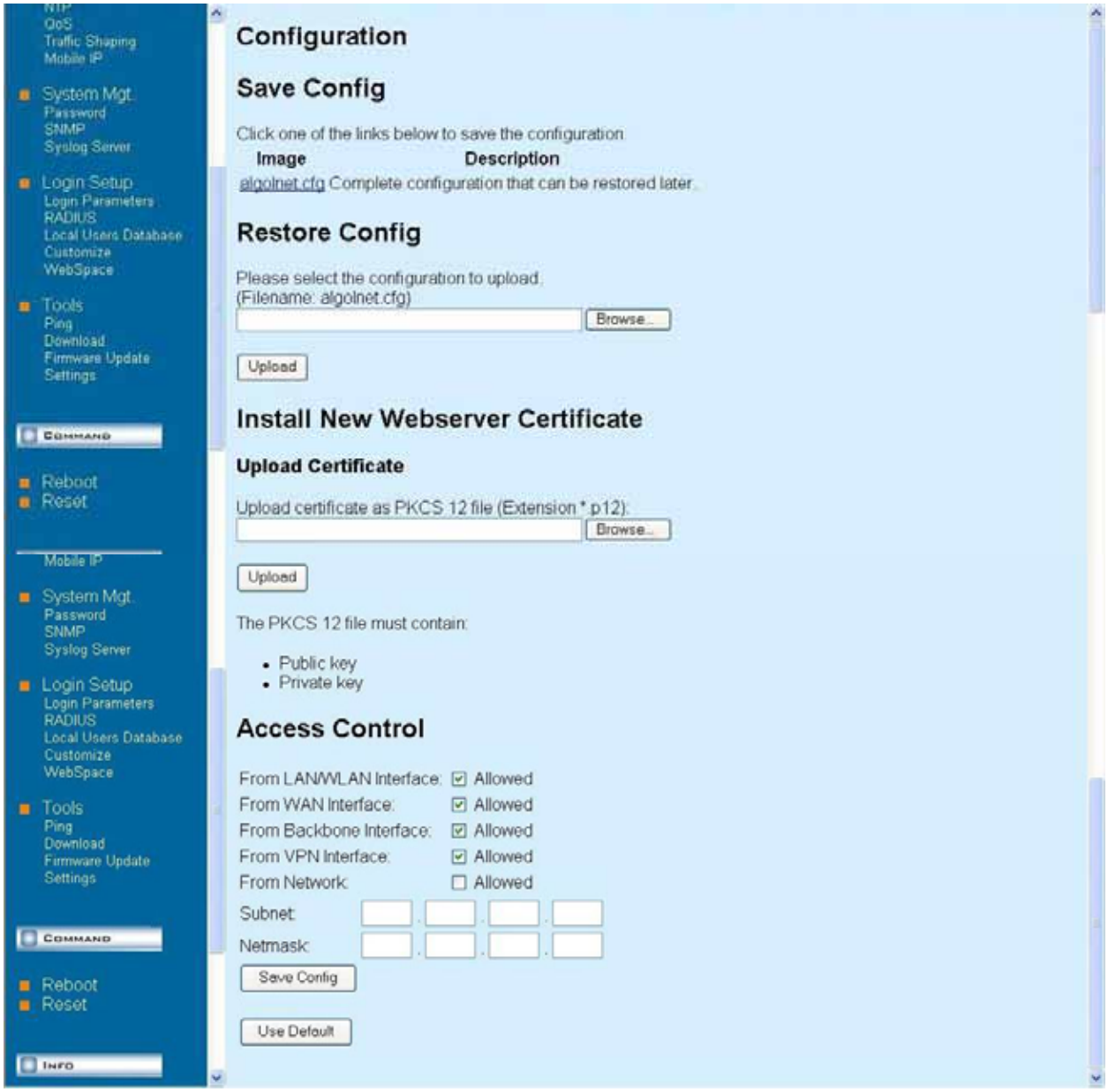
This option allows user to update the MESH AP firmware.
Caution! Please don’t switch off the device while updating the firmware. It may take average about **6** minutes to update the firmware.

Firmware Update Parameters:

- Click “Browse” button to browse to the location of new firmware and select that file
- Example: a:\firmware.img
- Click “Upload” button to upload the new firmware to MESH AP

During the process, the services will shutdown. After the firmware upgrade, the MESH AP will reboot. To know when will be process completed, simply set the MESH AP back to default before upgrade and ping the default IP address of the MESH AP. Once the reboot process completed, then the MESH AP will reply the ping.

2.3.27 Configuration->Tools->Settings



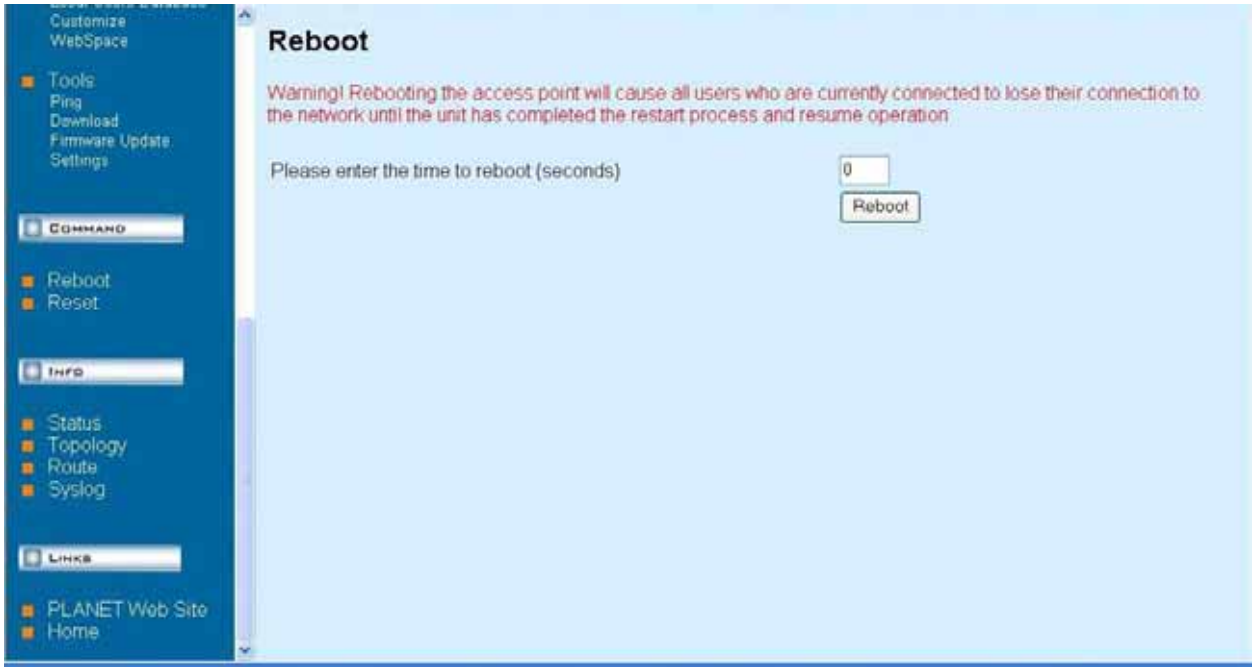
Configuration Parameters:

- Save Config
  - Save the configuration image to a file
- Restore Config
  - To update the MESH AP configuration with saved configuration
  - Click “Browse” button to browse to the location of new configuration image and select that file
  - Example: a:\MESH_AP1.cfg
  - Click “Upload” button to upload the new configuration.
- Install New Webserver Certificate
  - Install Web Server Certificate
    - Upload our web certification that certified by authorized Certificate Authority (CA)
    - Click “browse” button to select the certificate file from user designated source

- Click “Upload” button to upload certificate to MESH AP
- Example: webserver-mesh.p12

2.4 Command Menu

2.4.1 Command->Reboot



Reboot Parameters:

- Time to reboot
  - To specify a delay in time before rebooting.
- Click “Reboot” to initiate the reboot sequence.

2.4.2 Command->Reset

Reset Parameters:

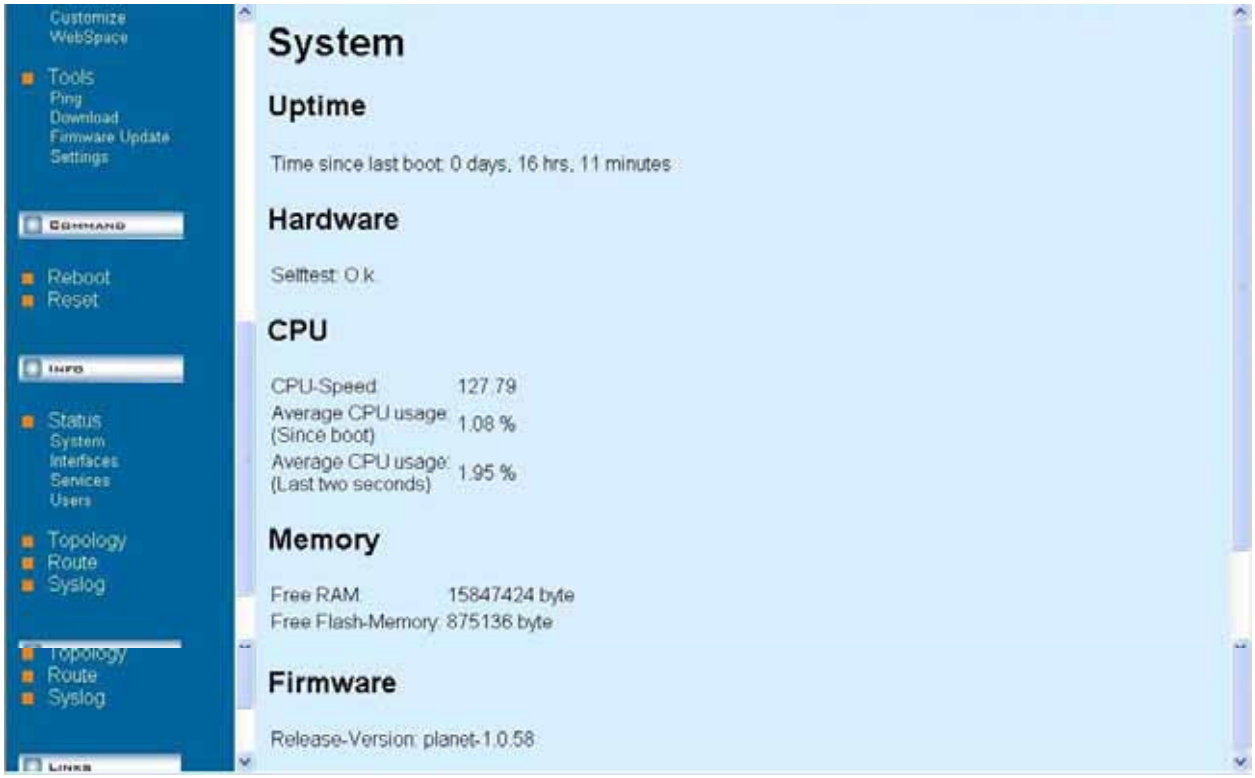
- Reset to Factory Default
    - To restore the default factory configuration
- Click “Reset to Factory Default” to restore to default factory setting

2.5 Info Menu

This menu allows the administrator to check the current status of various MESH AP components such as system, interfaces. It also helps to provide diagnostic tools to investigate the MESH AP behaviors.
Info menu consists of two submenus, which known as status, tools and topology. The following section will discuss each submenu in details.

2.5.1 Info->Status->System

The status menu displays the information of system, interfaces, services and existing login users details.

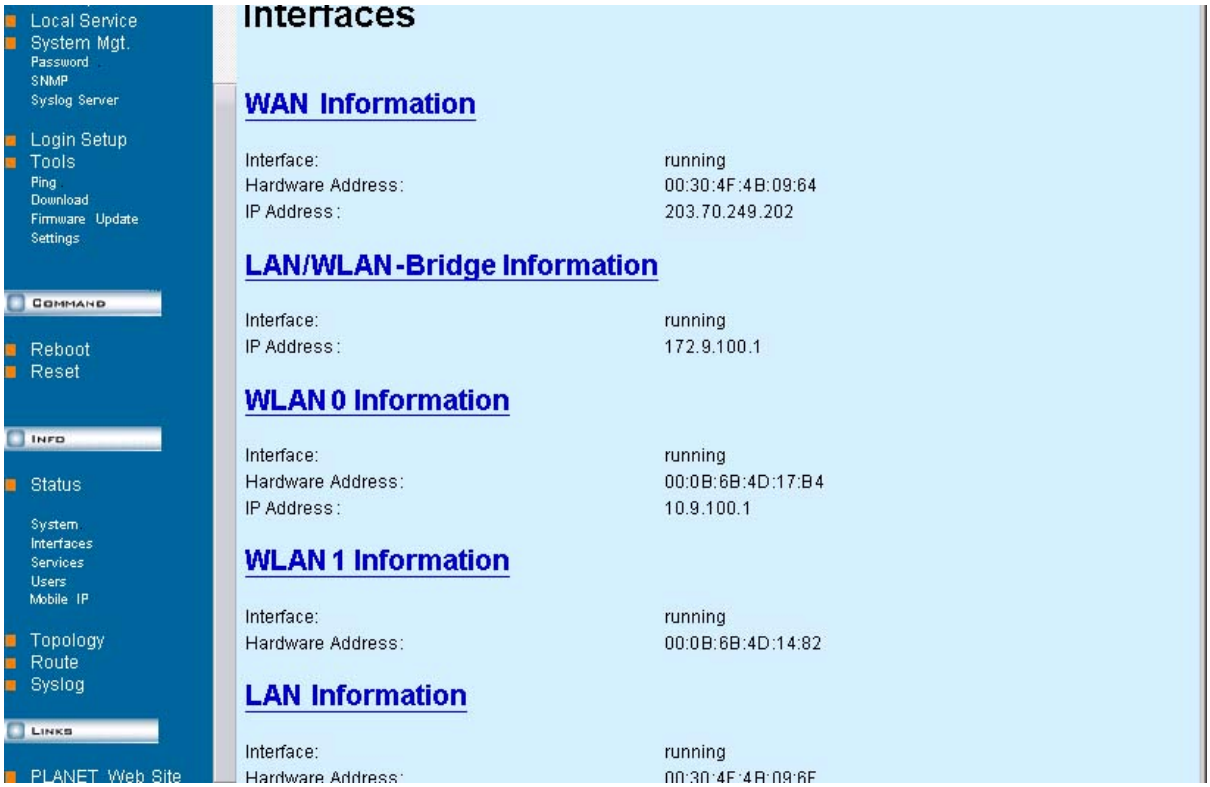


System Parameters:

- Uptime
  - Display the uptime in days/hours/minutes
  - Example: Time since last boot 0 days, 0 hrs, 34 minutes
- Hardware
  - Display the MESH AP self-test after boot
  - Value “OK” means self-test passed
- CPU
  - To display the MESH AP MPC 8241 Processor status
  - CPU-Speed
    - Display the MCP 8241 CPU speed
  - Average CPU usage (Since boot)
    - Display the CPU usage since boot in terms of percentage
  - Average CPU usage (Last two seconds)
    - Display the CPU usage of last two seconds in terms of percentage
- Memory
  - Free memory
    - Display the available free system RAM memory
  - Free Flash-Memory
    - Display the available free system FLASH memory
- Version
  - Secondary version
    - Display the current secondary firmware version
  - Tertiary version
    - Display the current tertiary firmware version

2.5.2 Info->Status->Interfaces

Display the LAN interface, WLAN interfaces and WAN interface general information.



Interfaces Parameters:

- WAN Information
  - To display the WAN interface general information
  - Click “WAN Information” link to display details information.
  - Interface
    - To display current state of the WAN interface
  - Hardware Address
    - To display the MAC address of the WAN interface
  - IP address
    - To display the IP address assigned to the WAN interface
- LAN/WLAN-Bridge Information
  - To display the LAN/WLAN Bridge interface general information
  - Click “LAN/WLAN Bridge Information” link to display details information.
  - Interface
    - To display current state of the LAN/WLAN Bridge interface
  - IP address
    - To display the IP address assigned to the LAN/WLAN Bridge interface
- WLAN0 Information
  - To display the WLAN0 interface general information
  - Click “WLAN0 Information” link to display details information.
  - Interface
    - To display current state of the WLAN0 Bridge interface
  - Hardware Address
    - To display the MAC address of the WLAN0 interface

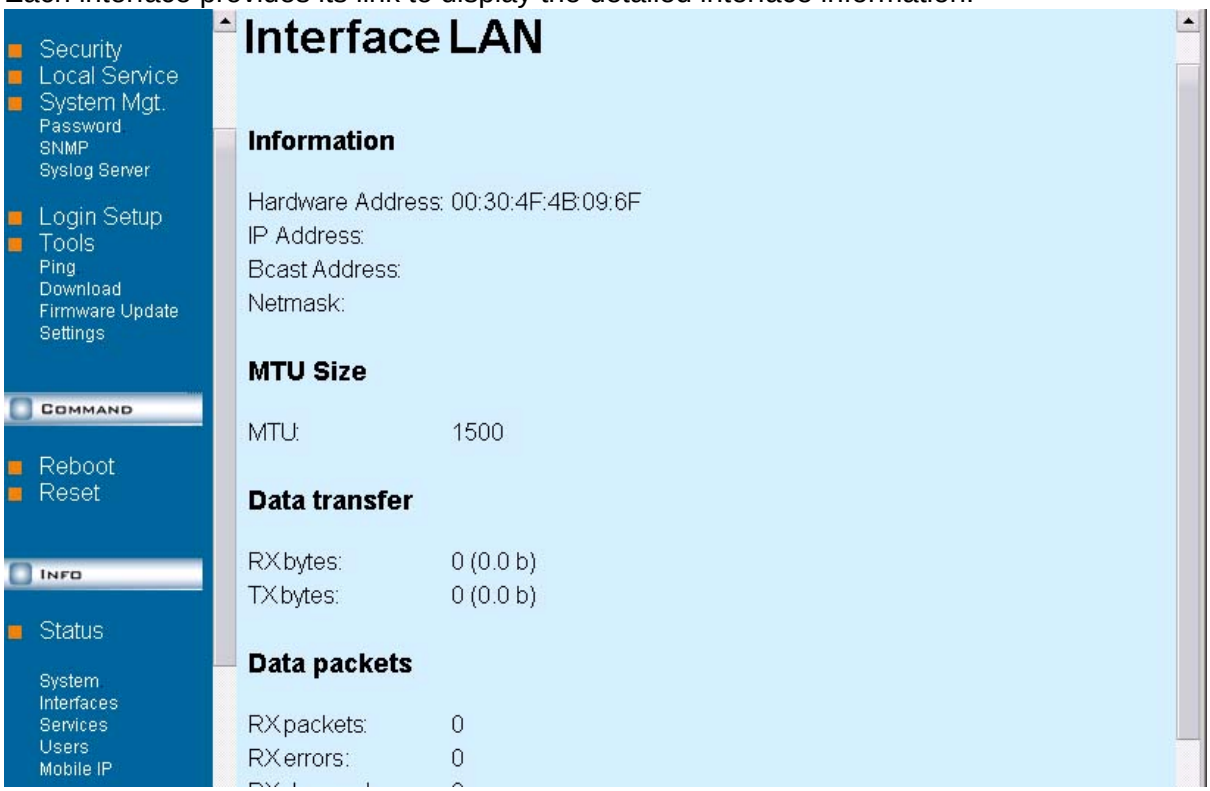
- WLAN1 Information

  - To display the WLAN1 interface general information
  - Click “WLAN1 Information” link to display details information.
  - Interface
    - To display current state of the WLAN1 Bridge interface
  - Hardware Address
    - To display the MAC address of the WLAN1 interface

- LAN Information
  - To display the LAN interface general information
  - Click “LAN Information” link to display details information.
  - Interface
    - To display current state of the LAN interface
  - Hardware Address
    - To display the MAC address of the LAN interface

2.5.2.1 Detailed Interface Information

Each interface provides its link to display the detailed interface information.

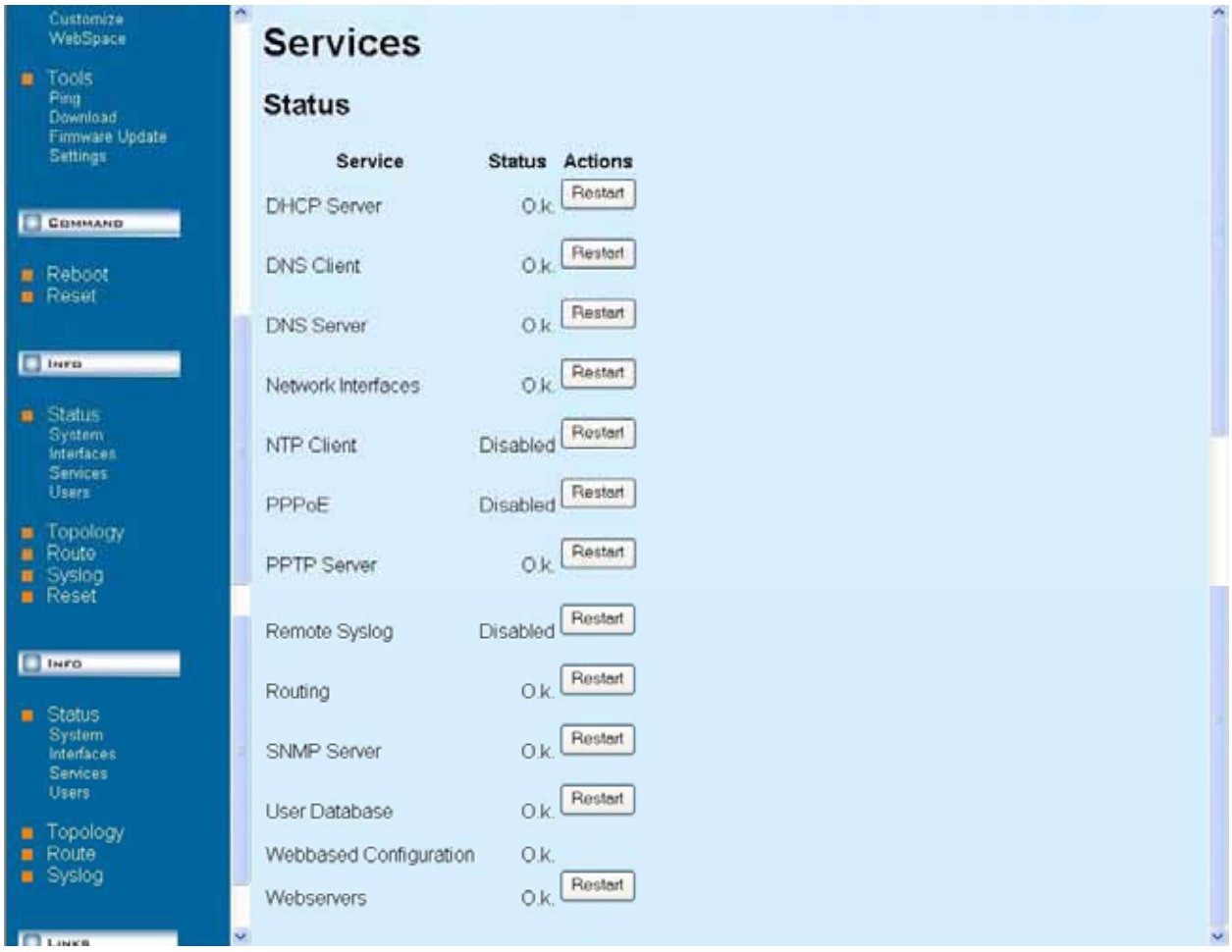


Interface Parameters

- Information
  - Hardware Address
    - Display the interface MAC address
  - IP address
    - Display the interface IP address
  - Bcast address
    - Display the interface Broadcast address
  - Netmask
    - Display the interface Netmask
- MTU Size
  - MTU

        - Display the interface Maximum Transfer Unit
- Data Transfer
    - Rx bytes
        - Display the received bytes on the interface
    - Tx bytes
        - Display the transmitted bytes on the interface
- Data Packet
    - Rx packets
        - Display the received packets
    - Rx errors
        - Display the received error packets
    - Rx dropped
        - Display the received dropped packets
    - Tx packets
        - Display the transmitted packets
    - Tx errors
        - Display the transmitted error packets
    - Tx dropped
        - Display the transmitted dropped packets

2.5.3 Info->Status->Services



Services Parameters:

- Status
    - Display current status of various service configured and running

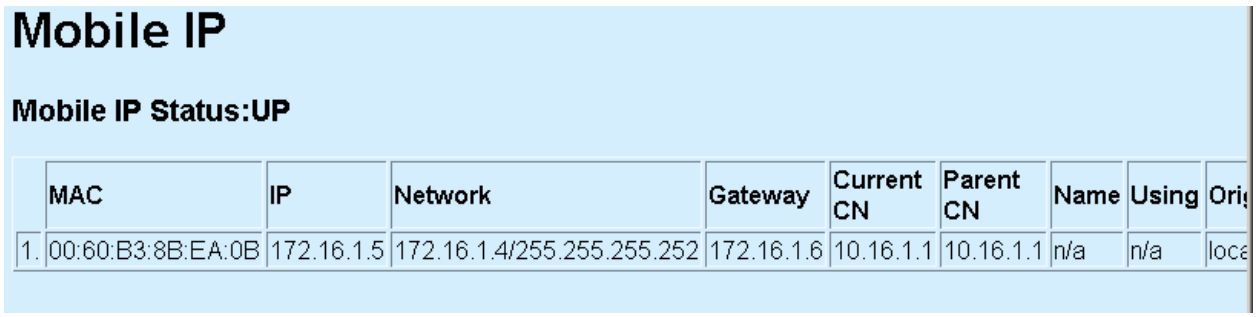
- Click “Restart” button to restart the selected service

2.5.4 Info->Status->Users

Online Users Database Parameters:

- List of Users
  - Display the current logon user list
  - User name
    - Display the logon user name
    - Click this link to display the user details
  - IP address
    - Display the IP address assigned to the logon user interface
  - Actions
    - Click “Logout” button to logout the user manually

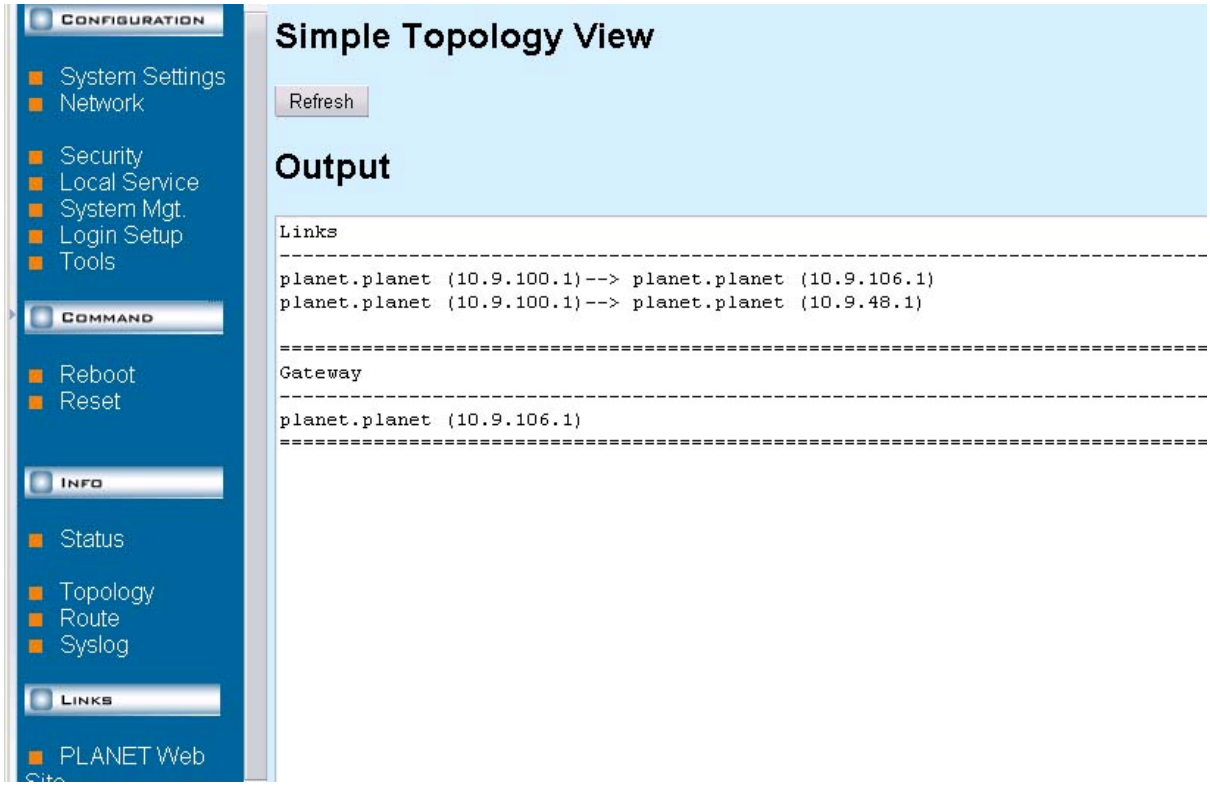
2.5.5 Info->Status->Mobile IP



Display the status of the mobile IP status

2.5.6 Info->Topology

Display the current topology of the mesh network.

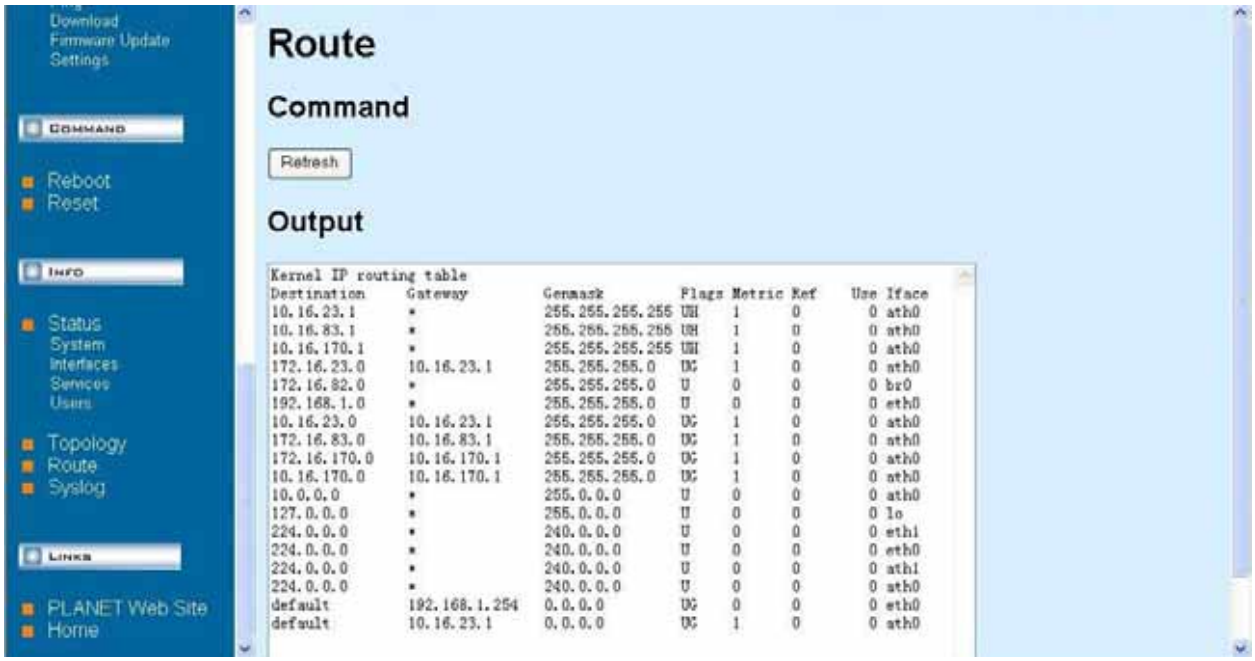


Topology Parameters:

- Click ‘Refresh’ to obtain the current mesh network topology.
- Output

2.5.7 Info->Route

Display the MESH AP IP routing table.



Route Parameters:

- Click ‘Refresh’ to obtain the current IP routing table information.

- Output
    - Display the current IP routing table interfaces information

2.5.8 Info->Syslog

To view the system messages and significant events that occur on the MESH AP.

Download
Firmware Update
Settings
COMMAND
Reboot
Reset
INFO
Status
System
Interfaces
Services
Users
Topology
Route
Syslog
LINKS
PLANET Web Site
Home
Syslog
Command
Refresh
Output
May 2 08:00:15 gateway syslog.info syslogd started: BusyBox v0.60.0 (2006.01.13-01:33+0000)
May 2 08:00:15 gateway user.notice hap: Starting ntpd
May 2 08:00:16 gateway user.notice hap: Starting webservers
May 2 08:00:18 gateway user.notice hap: Configuring iptables rules
May 2 08:00:19 gateway user.notice hap: Setting user defined firewall rules
May 2 08:00:19 gateway user.notice hap: Starting Radius Client
May 2 08:00:19 gateway user.notice hap: Starting RADIUS client
May 2 08:00:19 gateway user.notice hap: Enabling routing (ip_forward)
May 2 08:00:20 gateway user.notice hap: Starting DHCP
May 2 08:00:20 gateway local0.info dhcpd: Internet Software Consortium DHCP Server 2.0pl5
May 2 08:00:20 gateway local0.info dhcpd: Copyright 1995, 1996, 1997, 1998, 1999 The Internet Software Consortium.
May 2 08:00:20 gateway local0.info dhcpd: All rights reserved.
May 2 08:00:20 gateway local0.info dhcpd:
May 2 08:00:20 gateway local0.info dhcpd: Please contribute if you find this software useful.
May 2 08:00:20 gateway local0.info dhcpd: For info, please visit http://www.isc.org/dhcp-contrib.html
May 2 08:00:20 gateway local0.info dhcpd:

Syslog Parameters:

- Click ‘Refresh’ to obtain the current system logging information.
- Output
    - Display the current system logging information.

- o

2.6 Links

This menu provides the HTML links to the MESH AP main webpage and PLANET homepage.

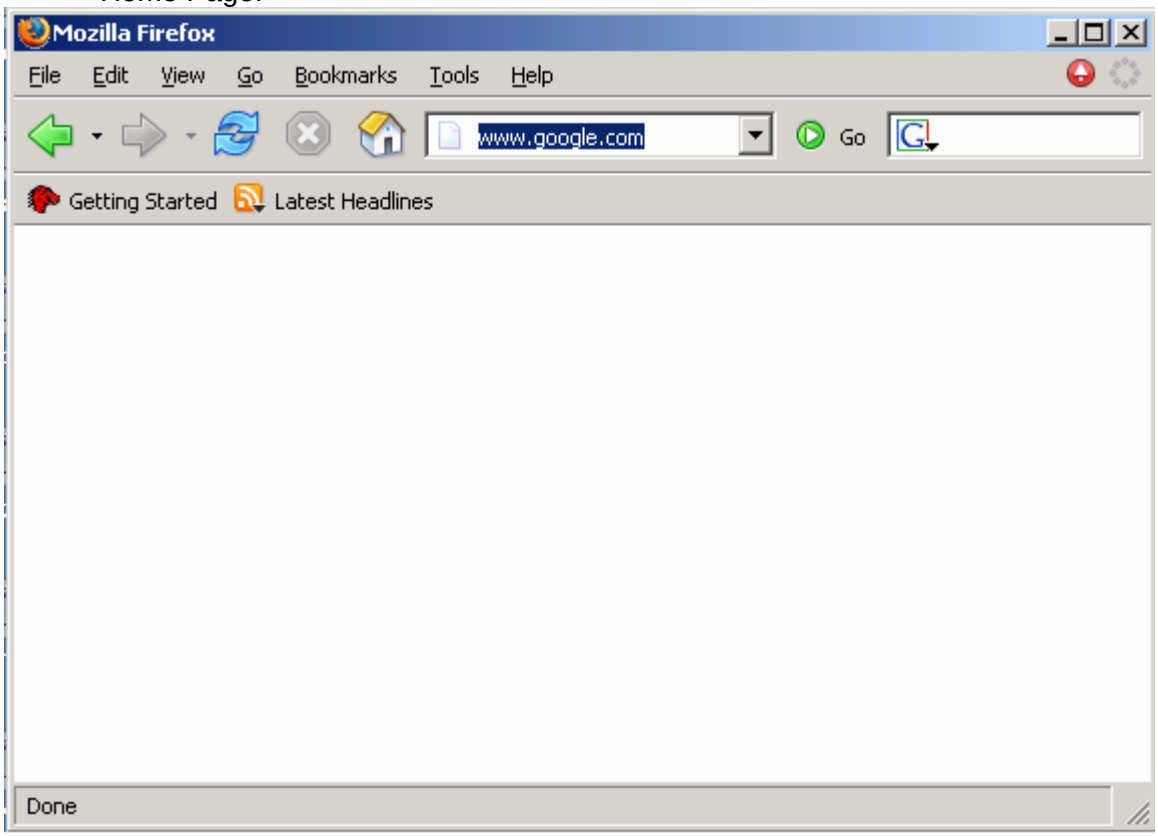
Click the link to access the respective web page.

3 Logging in through MESH AP

This chapter describes the basic steps to use the MESH AP service.

Step 1: User Starts WEB Browser

- User is ready to access the Internet and starts Web Brower and requesting default Home Page.



Step 2: Login Page Presented to User

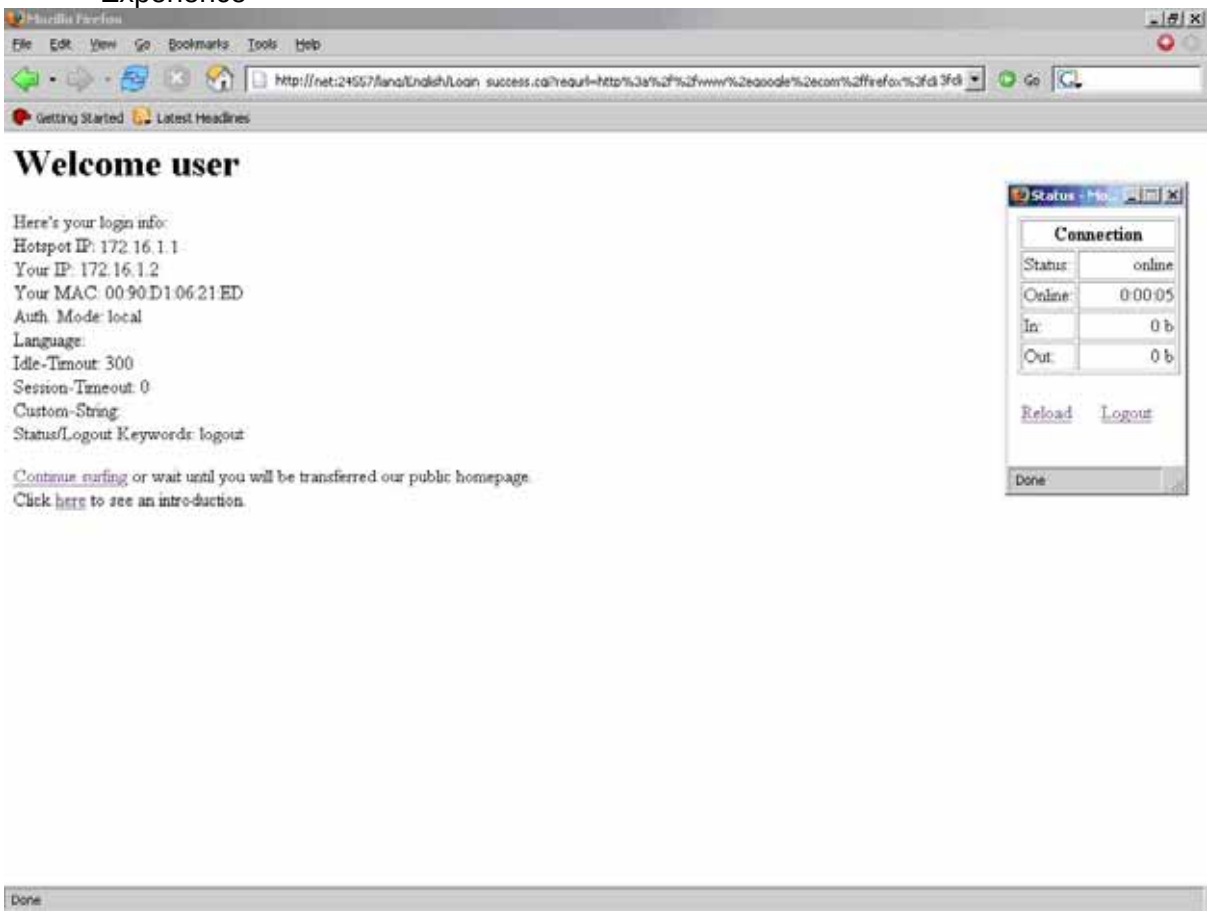
- Connecting to the Service
- The requested “Home Page” is intercepted by MESH AP and replaced by a User Login Page
- The Login Page is protected by SSL (HTTPS)
- CA Certificate is automatically downloaded prior to accessing the Login Page
- Note: PDA Users can use HTTP (Non-SSL) Login

Step 3: User Supplies Credentials

- Logging On
- User supplies his/her ID and Password to access the Internet
- User Credentials are validated against RADIUS Server

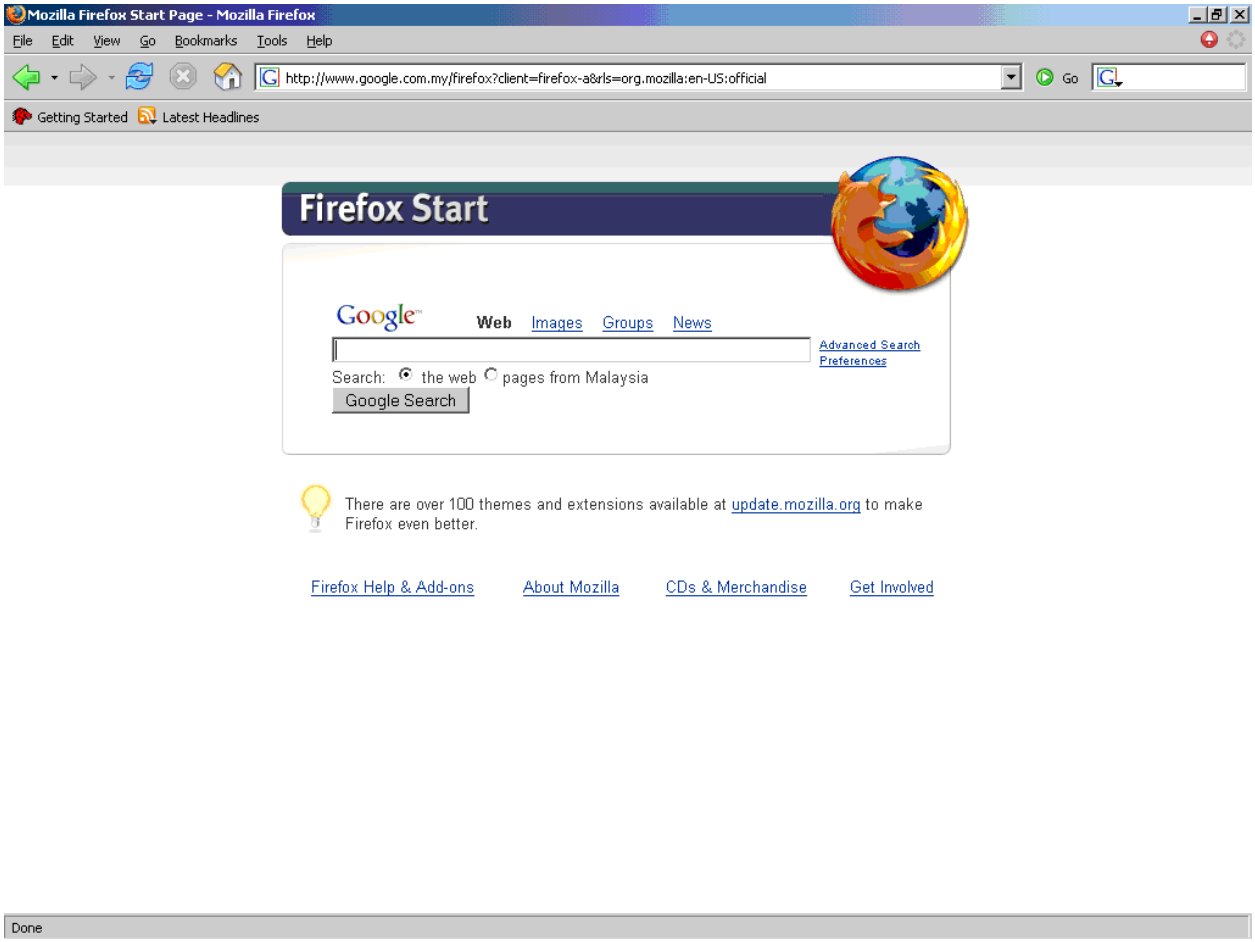
Step 4: User Login Success

- Welcome Page
- Upon Successful Authentication and Authorization, the MESH AP ISP can present user with User and/or Location specific “Welcome Page” to further the User Experience



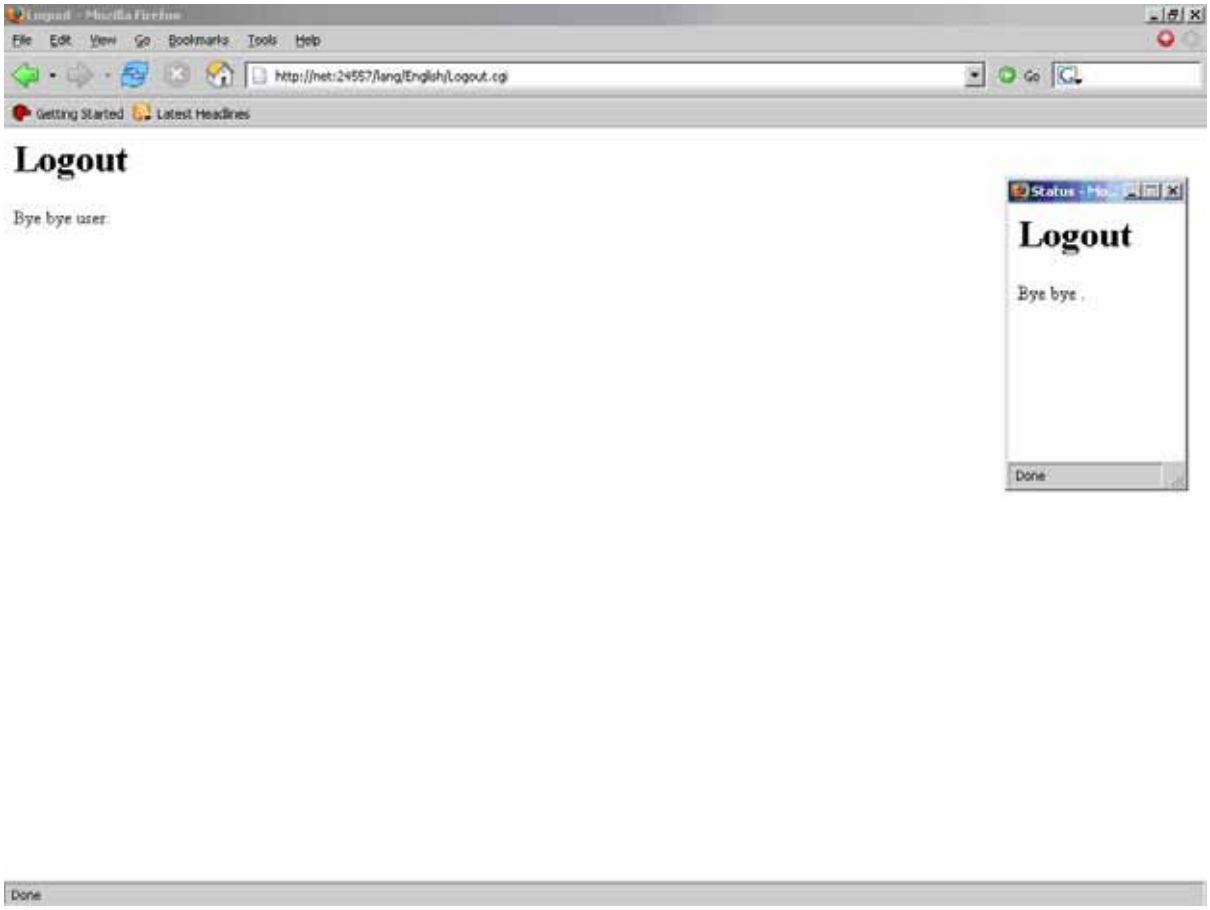
Step 5: Display the Request Home Page

- After the “Welcome Page”, User is now presented with the Home Page initially requested and is now ready to surf the Net
- A “Session Page” is now displayed to User with information on
- Duration of Usage
- Capacity of Data Transfer
- Time-Left for Prepaid System, or etc



Step 6: User Logout

- Once User is done accessing the Internet or the remote Corporate Network, the Session Page is used to Logout
- A simple Click on the “Logout” button
- For Pocket PC System just type in “Logout”
- Logout can also happen under control of the Wireless Operator or when the time-credit on prepaid system is expired


File Edit View Go Bookmarks Tools Help
http://net:24557/lang/English/Logout.cgi
Getting Started Latest Headlines
Logout
Bye bye user.
Logout
Bye bye .
Done
Done